Wireless Personal Communications (2019) 104:1599–1636
https://doi.org/10.1007/s11277-019-06120-8

Novel Trust Based Energy Aware Routing Mechanism for Mitigation of Black Hole Attacks in MANET

R. Tino Merlin[1] · **R. Ravi**[1]

Published online: 6 February 2019

Abstract
The open transmission characteristics in wireless environments and scarce energy resources generated many challenging factors in MANET's. Presently, MANET's are highly employed in security related applications. Moreover, security problems and energy efficiency are considered as the supreme factors in MANET whereas, the security threats emerges out due to their scare resource characteristics; hence their functionalities are highly degraded with numerous security attacks namely, the cruel black hole attack (BHA). The BHA mainly distresses the data collection and makes an effort to engage in most of the links as possible to increase the resource constrained issues in the network. In order to withstand these issues, we propose a novel trust based energy aware routing (TEAR) mechanism for MANETs. The most important characteristics of TEAR mechanism is that it mitigates BHs through the dynamic generation of multiple detection routes to detect the BHs quickly as possible and provides better data route security by obtaining the nodal trust. More significantly, the TEAR mechanism can effectively handle both the creation and sharing of these multi-detection routes for the detection of BHs. Essentially, these multi-detection routes in TEAR mechanism are generated by wholly utilizing the energy in non-hotspots (i.e. without wasting the energy) to improve the energy efficiency and desired data route security. The theoretical and experimental analysis proved that our TEAR mechanism exhibited better performance than that of the earlier research works. The TEAR mechanism highly optimizes the lifespan of network by avoiding the black hole attacks and drastically increasing the probability of successful data routing.

Keywords Trust · Energy efficiency · Security · Black hole attack · MANET · Network lifespan

✉ R. Tino Merlin
tinophd@gmail.com

[1] Department of Computer Science and Engineering, Anna University Recognized Research Centre, Francis Xavier Engineering College, Tirunelveli, India

1 Introduction

Wireless networks are the popularly known user convenient network, in which the nodes can move affordably without requiring the support from cables or from extensive infrastructure [1–3]. More specifically, the wireless network is composed of two main components namely, (1) wireless clients and (2) access point (or a wireless router) [4]. The advantages that relays on wireless networks are, low cost, expandability, easy setup, mobility and convenience [5]. Specifically, the wireless networks exists in different forms such as, MANET (Mobile Ad hoc Networks), WPAN (Wireless Personal Area Network), WLAN (Wireless Local Area Network), WWAN (Wireless Wide Area Network) and so on [1, 6]. In general, MANETs are recognized by the following characteristics such as, free movement of nodes in the network, scalability, high degree of user's mobility, high user density, shared physical medium, light weight terminals (especially, memory, power consumption), no centralized point, multi-hop routing, limited security, and dynamic topology [7–10].

On the other hand, MANET is a network comprised with wireless devices and when required these wireless devices can exchange information with each other. Consequently, the MANET nodes work on the basis of three different modes such as, communication, computation and sensing. It should be noted that, the sensing-mode intakes minimum energy (battery) while the communication mode consumes more energy for processing the communication. In order to compensate the energy scarcity, there is in need to construct an effective routing protocol for MANETs. The primary goal of any routing protocol is to establish an optimal and efficient route between the communicating nodes. From the past decades, much research[2, 3, 11] efforts have been focused on this area and many different kinds of routing protocols have been put forward in the existing studies, such as Wireless Routing Protocol (WRP) [4], Dynamic Source Routing protocol (DSR) [5], Ad hoc On Demand Distance Vector protocol (AODV) [6] and Location Aided Routing [7]. However, from the beginning of its design, almost none of the routing protocols specify security measures.

To implement Security in MANETs is a complex issue. Nodes in the network are much more vulnerable to attacks compared to wired (traditional) networks due to the open medium, dynamically changing network topology, lack of centralized monitoring and management point, and lack of a clear line of defense. On the other hand, MANET is an infrastructure less network where the clients can move freely without any restriction. Due to this fact, the network topology shows dynamic and frequent changes with free nodal mobility. Moreover, the MANETs emerge as a potential expertise due to their challenging applications in civilian and military areas, environmental monitoring and industrial innovations [1, 4–8]. The nodes are deployed freely because they are low cost and simple. Beyond this effectiveness, they are not so much potential to fight against different types of malicious attacks [8–10]. However, several security attacks emerge due to such specific characteristics of MANETS. One such kind of attack is a black hole attack [4, 7].

Most well-known MANET routing protocols [12, 13] use a deterministic strategy to discover routes to a destination node and then use this route until the route breaks or a better route is discovered. In scenarios where the black hole attacker is present between two communicating nodes, this behaviour can lead to an undesirable situation where the MANET routing protocol is frequently switching between multiple available routes even though the topology of the network did not change, which may result in uneven load distribution, network instability and reduced traffic throughput [9]. This problem is often denoted as "route flapping" [14]. Route flapping can be a significant problem, since it

affects not only the end-to-end network performance but can also lead to imbalanced use of the resources on the MANET nodes. To overcome this problem, Instead of selecting only one route, multiple routes could be used in parallel. This approach is generally called multipath routing and has been studied before.

In black hole attack (BHA), the malicious nodes try hard to enter into many dynamic (active) links for establishing the scarcity of resources in the network. The working procedures of BHA [14] are as follows: A node is compromised by an adversary and all the packets that are routed through this node are dropped; hence the packets are incapable to be transmitted to the sink or results in loss of sensitive data. It should be noted that, nodes are meant with sensed data and only based on this sensed data the network generates the decisions. Due to this fact, the network may generate incorrect decisions with serious network failure [15–20]. Consequently, these issues create a significant security based challenge in MANET (i.e. how to detect and avoid BHA).

Various literal works conducted an investigation on black hole attacks [14, 21–24]. Such examinations mainly focused on the heuristics of Black Hole (BH) avoidance [14, 23]. Some of the approaches similar to [24], doesn't demand for the prior knowledge about the black hole. These studies exhibits that the packet is broken into N shares and the divided shares are transmitted through multi-path (different routes) to reach the sink. The transmitted packets are possible to be resumed with t shares (i.e.$t \leq N$). The inadequacy met with these approaches is that, the sink receives more number of shares than the requested number of t shares. As a result, the sink intakes more energy (leading to high energy consumption) to process these received shares and leads to scarcity of resources [14, 22]. Moreover, trust route strategy is the most preferable strategy to enhance the route success probability. Numerous related works were performed with this trust route strategy [25–29].

The main aspect that relays on the trust route strategy is to generate a route by choosing the nodes with high trust; hence, the nodes with maximum trust measure can have a higher probability of successful routing. As a result, the routes generated based on this behavior can transmit data to the base station/sink with maximum successful routing probability [27, 28, 30]. However, there exist few challenging issues with the trust-based routing and other on-demand routing strategies exposed in [12, 13, 31, 32]. Some of the challenging issues are as follows: (i) *Trust:* the primary goal of trust route relays on obtaining trust. More importantly, obtaining a node trust is a most complex process and it is still unclear about the way that it can be performed. (ii) *Energy efficiency:* From the past research works, it is possible to infer that MANET's energy consumption is more with diffusion and trust acquisition, which may critically influence the lifespan of the network. (iii) *Security:* the secure routing is still an open issue with the trust based routing and on-demand routing protocol, since they don't maintain routing information or routing activity at the network nodes if there is no communication. If a node wants to send a packet to another node then this protocol searches for the route in an on-demand manner and establishes in order to transmit and receive the packets. However, it operates with the assumption that all participating nodes are well-behaved, and thus, it does not include any security mechanism. In other words, it is hard to locate the malevolent nodes. Furthermore, there exist more valuable security and trust concerned issues with further examination. In this work, trustable and secure routing is achieved through a dynamic multi-detection routing protocol. *The main findings of our work are as follows:*

(a) The TEAR mechanism is the one and most routing mechanism that exploits the *dynamic multi-detection* routing to handle the Black Hole Attack (BHA).

The most significant effect that can be observed with TEAR mechanism and former research works [12, 13, 31, 32], is that we generate number of detection routes in regions with residual energy. This is due to the fact that, the black hole attacker is not so much aware about the detection routes; hence the attackers will attack these routes and during such activity, the route attackers are exposed. In such a way, the location and behavior of attackers as well as the node trust can be obtained. However, while executing real data routes these obtained information can be used to ignore the black holes. To the best of our knowledge, this is the most magnificent routing mechanism in MANET.

(b) The TEAR mechanism obtains better energy efficiency.

Energy is the most valuable constituent in MANETs and when dynamic detection is performed the network loses its energy with further execution. However, in the former research, it was impractical to construct such type of high energy consumption dynamic detective routes. However, after analyzing the energy intake in MANETs, we observed that it is possible to perform dynamic multi-detection routing on the network. This fact is accomplished because, after analyzing the energy consumption in MANETs the previous study has delineated that there still remains 91% residual energy in MANETs even with the network death occurred due to the crucial energy hole phenomenon. Therefore, the TEAR mechanism can create multi-detection routes by considering the whole goodness of the residual energy left in the network and tries to minimize the energy consumption in hotspots with an end goal to improve the lifetime of the network. Also, the created multi-detection routes enhanced the network security by finding the nodal trust without minimizing lifetime. More significantly, theoretical and experimental analysis is performed with the TEAR mechanism and when compared with the conventional routing mechanisms such as multi-path, shortest routing, our proposed TEAR mechanism exhibits better energy efficiency. In other words, energy efficiency of the TEAR mechanism is enhanced more than two times compared to the traditional routing techniques, including multi-path routing [33, 34] and shortest path routing [35, 36].

(c) The TEAR mechanism obtains superior security performance.

When compared with earlier research, the TEAR mechanism dynamically obtains the nodal trust. The multi-detection route is generated with the following rules: Initially, to neglect the high potential attack, the nodes with maximum trust are selected and then the nodes are routed over a victorious (successful) detection route. Thus, with the above delineated approach, the network security is highly enhanced.

(d) Finally, through our broad theoretical and experimental analysis, we observed that our proposed TEAR mechanism possesses the ability to improve the "probability of success routing" (i.e. 1.5–6 times) and improves the energy efficiency (i.e. more than two times) contrasted with that of the earlier researches.

The rest of this paper is summarized as follows: Sect. 2 detailed the review of related works. Section 3 describes the system model formulation of the proposed approach. Section 4 describes the proposed TEAR mechanism and analyzed the effectiveness of the proposed approach with security and energy efficiency. The detailed description about the experimental analysis and comparative results are discussed under Sect. 5. Finally, the paper ends up with the conclusion and future enhancement in Sect. 6.

2 Review of Related Work

Most of the literal works focused only on the analysis of network performance with the entrance of malicious nodes and they maintained analysis without providing any better solution. However, to fight against BHAs (Black Hole Attacks) on MANETs several protocols and approaches occupied a major role. In [15], the authors conducted various examination on different types of security attacks such as gray hole attack, packet drop attack and black hole attack against different parametric measures which are commonly applied to evaluate the efficiency of the network performance (e.g. end to end delay, packet drop rate, throughput and so on).

From the analysis, it was observed that black hole attack is the serious security attack that highly degrades the data route security. The authors in [16], introduced a technique to identify the most secure routes and to avoid the malicious nodes (black hole nodes) in the MANET by evaluating the sequence number variations in the source node. On the other hand, it checks whether the intermediate nodes has transmitted RREP in the first stage or not. The technique in [16], maintained the RR table to store the nodal information. Initially, in the first entry of the table the route reply obtained from the malicious node is stored. The malicious node is ready to supply the initial route reply with maximum destination sequence number. Then comparative analysis was done with the sequence number of source node and with the initial destination sequence number. If the difference between the sequence numbers is in higher degree, then it was recognized that the sequence number is generated from the malicious node. After identifying the existence of malicious node, then it turns to be essential to eliminate them from the RR-Table. But the technique [16], fails to identify multiple BH nodes.

Mostly, the mobile devices are equipped with different kinds of sensors as similar to the mobile ad-hoc networks. In order to maintain better communication with the remote destination, the mobile node is in demand to transmit the packets to other mobile nodes and especially this criterion was highly focused on the multi-hop wireless networks. In case, the mobile nodes are malfunctioned through certain malicious activities then that particular mobile nodes takes a charge to drop the packets continuously and the data transmitting routes were broken because of the failure of software/hardware functionalities. Also to disrupt the transmission process, the malicious node vigorously breaks the routes [16, 18]. The transmission of packets in multi-hop networks is highly encouraged with the routing mechanism and this, in turn, enhances the spectral efficiency and broadens the networks communication range.

More significantly, limited battery power is the main inadequacy addressed by the nodes of mobile ad-hoc networks. Therefore, energy is the serious issue that should be resolved in MANETs for effective transmission of data to the mobile station [14]. The authors in [15, 16, 20] proposed many algorithm to resolve the energy resource constrained problems. In [18], the authors developed the Energy-Efficient routing protocol for MANET with load distribution approach. The major goal of this approach is to equalize the energy utility of the mobile nodes with proper selection of the routes from the non-utilized nodes instead of choosing the shortest-path.

In [22], the authors proposed a simple routing protocol referred to as single-path routing and the attackers can easily block this protocol to make them ineffective for further transmission of data. Hence the multi-path routing [23] is considered as a well effective approach for routing the data to the sink. The attackers can spoil only certain limited routes; therefore the data can be safely transmitted without any interruption. More commonly, two

classes were employed in multi-path routing protocols. These two classes were classified based upon the packet partition. The first class is referred to as routing without shared partition (i.e. packet is not divided into shares). The next subsequent class is referred to as routing with shared partition (i.e. packet is divided into shares).

Without Share-Division The creation of multi-path routing is of different forms. In [24], the authors developed a Multi-data flow technique to fight against the selective forwarding attack. In this technique, the network is partitioned into two set of topologies. If the malicious node enters into one of the topology, then the packets can be obtained from the next subsequent topology. In such protocols, the deficiency is that if the packet is routed through m number of routes simultaneously, the energy consumption will be *m* times higher that of a single path route, which will seriously degrade the lifespan of the network. These inadequacies can also be effectively seen in some of earlier multi-path routing protocols such as AODMV [32], AOMDV [25], and DSR [24].

With Share-Division The authors in [26] developed the SPREAD algorithm, in which they perform the multi-path routing with typical shares. The goodness behind this algorithm is that, each path can route only a single share and the attackers loses its ability to attack the nodes and the nodal information are secured in most efficient manner. The security and the privacy of the network are largely enhanced with this algorithm. But, in case, the routing algorithm is acquired from the adversary [19], then it paves the way for numerous attackers to decrease the routing efficiency. To resolve these issues, the authors in [27] developed four random propagation criterions and they are as follows, 1) MTRP (multicast tree assisted random propagation), NRRP (non-repetitive random propagation), DRP (directed random propagation), and PRP (random propagation). In this approach, the messages are initially partitioned into N number of shares and neglects to predetermine route/path of each share. Therefore, if the routing algorithm is obtained by the adversary, none of the attackers can affect the network because, the attackers fails to capture more number of shares [37, 38].

In MANETs to perform the multi-one data collection, we argue for the multi-path routing technique. The shares can be passed simultaneously through the similar path and this path is highly focused by the black hole attacker. The authors in [28], proposed the SEDR (Security and Energy efficient Disjoint Route) approach to improve the multipath routing with surplus energy. Moreover, trust routing is another effective routing strategy to improve the network security by avoiding the security attackers. In order to resolve those challenges in ad-hoc networks, trust management strives as a new force [29]. The TARF (trust-aware routing framework protocol) proposed by Zhan et al. [39], generates the route decisions through computing the cost and energy of the routes. Furthermore, depending upon the nodal functionalities, different trust computational techniques were developed by Sec-CBSN algorithm [40]. The Retrust mechanism is developed by the authors in [41], to improve the trust management performance of the MSNs (Medical Sensor Networks). The selfish or malicious node that affects the VANETs (vehicular ad hoc networks) performance by spreading the misleading information to the network can be quickly and accurately identified by the TRIP mechanism of [42].

More commonly, the trust value is evaluated depending upon the prior communications made between the devices and to make easier the study in pervasive computing the authors in [43] proposed the probabilistic trust management approach. In order to establish trust value among the nodes the trust vote is developed by the reputation based trust management mechanism in [44]. Furthermore, with every effectual data transmission the

trust vote value is augmented and for ineffectual data transmission the trust vote value is reduced. In [45], the authors developed two more convenient energy aware routing protocols referred to as SRR (Shortest Reliable Rout) and BAR (Best Available Route). These protocols are mainly employed to establish most reliable route to minimize the linkage breaking occurred due to energy constrained issues, malicious attacks and so on. The DSR (Dynamic Source Routing) protocol is utilized in the study of [46], to increase the probability of packet forwarding with trust based routing. In this, the routing protocol evaluates the number of forwarded and dropped packets using the trust measure of the nodes. However, the trust values obtained are updated to maintain a strong relationship between the nodes by the routing approach [47]. The approach in [48], evaluates the trust values of both the neighbors and the routing path by means of considering alone the packet forwarding (i.e. a single parameter).

However, many of the above delineated works have mainly focused on the avoidance of black hole nodes, but there still exists much more valuable study. (i) The lifespan of the network is highly degraded with the existing BH avoidance approaches. (ii) Most of the BH avoidance strategies severely affect the network performance because, they are passively acting systems. (iii) The guiding significance is limited due to high expense and complexity in obtaining the appropriate trust value with the former trust route mechanism [13, 49].

3 System Models and Problem Formulation

3.1 Network Model

A MANET is commonly built with group of mobile nodes which are interlinked by means of wireless links. All nodes in the MANET are connected with the nodes that are so much closer to the communication range. In MANET, direct communication to the destination node is not possible; thereby a source node first transmits the data to the intermediate (neighbor) node and then the intermediate node sends the data to the destination node. As similar to the wired network, the intermediate (neighbor) node takes a role of a router. More specifically, the security protocols that relates to the wired network are mainly applied in the router node. But, in MANET security implementation is considered as a most challenging task due to its hop-to-hop transmission of data to the sink (base station) (i.e. node itself will be acting as a router node). So identifying neighbor node as a legitimate node or malicious node is a difficult thing in MANET shown in Fig. 1. In order to maintain proper communication in the network, nodes should co-operate well for better transmission of data; hence the network communication entirely depends upon the trust of nodes. Also, when compared with the infrastructure-based wireless networks, the MANET usually suffers from more security threats as they fails to possess the fixed infrastructure. More importantly, in MANET due to its active (dynamic) nature, scarce resources (i.e. similar to battery power and bandwidth), and centralized monitoring has embedded lots of attacks in each of the communication layer.

(a) In this work, we assume a MANET consisting of mobile nodes which are connected one to one with the nodes nearer in the communication range. The nodes are randomly distributed in a circular network. Consider the nodal density as μ and the communication network radius as r, respectively [50, 51]. A node will generate messages after the

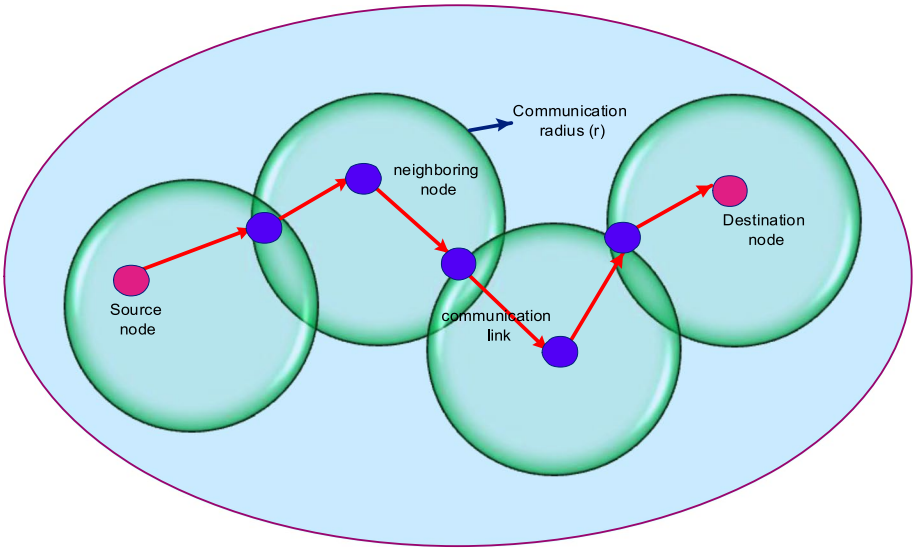

Fig. 1 Communication between nodes in MANET

detection of an event occurrence and the message from the source node is transmitted to the sink (base station) through communicating with the neighbor nodes.

(b) We assume that the cryptography based protocol has been commonly employed to establish the link-level security. Also, a link-key is considered as a safe measure, if not the opponent (adversary) tries to compromise either side of the link [51].

3.1.1 Adversary Model

We consider that the compromised nodes are responsible to form the black holes and these nodes will eliminate all the packets passed by to prevent data from being sent to the sink node [52]. The adversary has the ability to compromise some of the nodes. However, we consider the adversary to be unable to compromise the sink and its neighboring nodes [53]. We considered this, because an adversary has full control over the compromised nodes and can communicate with them at any time. In case of mobile ad-hoc network, the method of attack is the same but difference is that an adversary is mobile. The scenario of mobile networks is that the nodes are unable to transmit sensed data at their will because the sink (base station) is not always present. Thus, the data accumulated in their memories become targets of many adversaries. In other words, the mobile adversary visits and travels around the network trying to compromise a subset of nodes within the time interval when sinks are not present in the network. The time taken by a mobile adversary to compromise a set of mobile nodes is much shorter than the time between two successive data collections of

a sink. Therefore, in this work, we consider the adversary to be unable to compromise the sink and its neighboring nodes.

3.2 Model of Energy Consumption

It is generally known that energy is one of the most important resource factors in MANETs. Energy is needed to transmit, receive and handle the data. In this paper, we considered the energy model stated in [50, 51, 54], We assume that each mobile node has the same initial available energy level, whereas, Eq. (1) represents energy consumption for transmitting, and Eq. (2) represents energy consumption for receiving. e_{Elec} represents the transmitting circuit loss. Both the free space (p^2 power loss) and the multi-path fading (p^4 power loss) channel models are used in the model depending on the distance between the transmitter and receiver. $\in_{Fs}$ and $\in_{Amp}$ are the respective energy required by power amplification in the two models. In order to send a k *bit* packet through distance d, the energy consumed can be calculated using Eq. (2) (i.e. when a mobile node receives a k bit packets, the energy consumption is $e_r(k) = ke_{Elec}$). The parameter settings for the model are shown in Table 1.

$$\begin{cases} e_{member} = ke_{Elec} + k \in_{Fs} p^2 & if \quad p \le p_0 \\ e_{member} = ke_{Elec} + k \in_{Amp} p^4 & if \quad p > p_0 \end{cases} \tag{1}$$

$$e_r(k) = ke_{Elec} \tag{2}$$

3.3 Problem Formulation

We first describe the problem statements used in this proposed approach:

1. Network lifespan: It is defined as the time taken by the first node to die itself in the network [50, 51, 54, 55]. The lifespan maximization of node j with energy consumption e_j is expressed by the following equation:

$$Max(t) = \min_{\max}(e_j) \tag{3}$$

2. Moreover, better security performance is obtained with the data collection and possesses the ability to fight against BHAs (Black Hole Attacks).

Our proposed mechanism mainly aims to ensure that the transmitted packets without any drop in the link (i.e. not blocked by the black hole attack) reach the sink node. In other words, the design goal of our proposed mechanism is to maximize the probability of packets successfully reaching the sink node. Let us assume that, n be the number of packets that are required

Table 1 Parametric settings of the network

Parameter	Value
Initial energy	0.5 J
$\in_{Amp}$	0.0012 (pJ/bit/m^4)
$\in_{Fs}$	10 (Pj/bit/m^2)
e_{Elec}	50 (nJ/bit)
Communication range (r_C)	16 m
Threshold distance (t_{d_0})	85 m

to reach the destination node and N be the total number of packets that finally succeed in reaching the sink; therefore the successful ratio is estimated as follows:

$$R = n/N \tag{4}$$

The energy consumption e_j for node j computed by varying the number of nodes in the limit [0 to m], the lifetime maximization $Max(t)$ is evaluated and our goal is to increase (maximize) the success ratio and is represented as $Max(R)$. However, the optimization goal of this work is represented using the following equation:

$$\begin{cases} Max(t) = \min \max\limits_{0<j\leq m} (e_j) \\ Max(R) = n/N \end{cases} \tag{5}$$

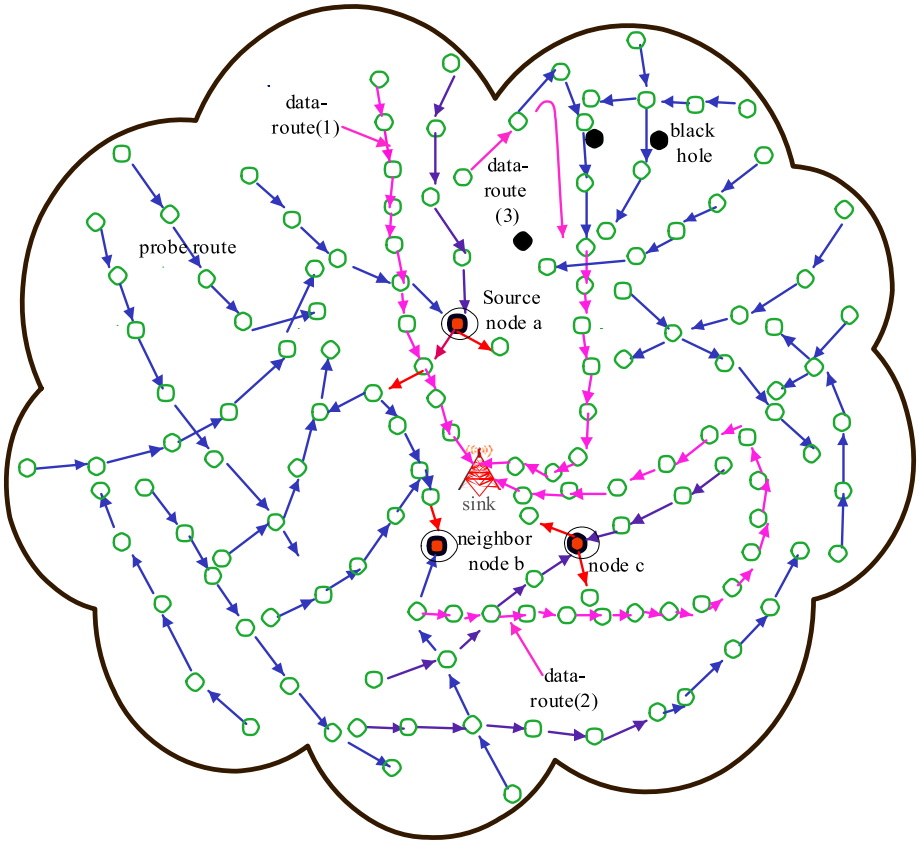

Fig. 2 Design of a TEAR mechanism

4 Design of TEAR Mechanism

An overview of the proposed TEAR mechanism is well illustrated in Fig. 2. The TEAR mechanism is developed with two routing protocols namely, *dynamic multi-detection routing* and *data routing* protocols.

4.1 Dynamic Multi-detection Routing Protocol

A route not including any of the data packets refers to a multi-detection route and the main target that relays on this detective route is to encourage the adversary to reach (launch) an attack. Thus, the system can easily find the attack behaviors and then points out the location of the BH (Black Hole). During this process, the system can lower the trust of suspicious nodes and increment the trust of nodes in successful routing routes. However, most of the well-known MANET routing protocols [12, 13] use a deterministic strategy to discover routes to a destination node and then use this route until the route breaks or a better route is discovered. In scenarios, where the black hole attacker is present between two communicating nodes, this behavior can lead to an undesirable situation where the MANET routing protocol is frequently switching between multiple available routes even though the topology of the network did not change, which may result in uneven load distribution, network instability and reduced traffic throughput. However, these hurdles in the existing routing protocols [12, 13] can be overridden effectively by our dynamic multi-detection routing protocol which can quickly obtain the nodal trust and it can successfully guide the data route to select the nodes with high trust to avoid the BHs (Black Holes). In Fig. 2, the dynamic multi-detection routing is shown via the blue arrow. The working procedures of dynamic multi-detection routing protocol are explained below:

4.2 Illustration of Dynamic Multi-detection Routing Protocol

In this, we detailed the implementation of the dynamic multi-detection routing protocol. Table 2 illustrates the algorithm of multi-detection routing protocol.

Initially, the source node randomly selects an undetected neighbor node to create a detection route. We consider ω as the largest route length and this route keeps on trying to minimize its length until it reaches to zero. In other words, the route length is decreased by one for every hop until the length is decreased to zero. Ultimately, the detection route ends after reaching the zero length. The multi-detection routing packet is divided into six parts (Fig. 3). (i) Packet-head, (ii) Packet-type, (iii) source node-ID, (iv) maximal length of the detection route, (v) Acknowledgement received by the source node for each hops (μ), (vi) Packet-ID.

Algorithmic Elucidation

- The source node (i.e. node a) selects an undetected node (i.e. neighbor node b nearer to the sink) to initiate the detection route.
- The nodes after receiving the detection packet, the maximum length of the route termed as $\bar{\mu}$ is reduced by one.
- Subsequent to this, a feed_back packet is generated with the criterion $\bar{\mu} = 0$ and a feed_back route is launched to the source node.
- Followed by this, re-establish $\bar{\mu}$ to the initial value.

Table 2 Pseudo-code of dynamic multi-detection routing protocol

1: Initialization
2: for each neighbor node a_n do
3: Let a_n.Acess_time=Current_time
4: End for
5: for a detection packet created by each node (i.e. for node a), do
6: do value assignment for μ and $\overline{\mu}$ by constructing a packet P_{kt}
7: Choose node b as the next hop node whereas, the node b consumes minimum Acess_time and it is largely closer to the sink.
// node b is the nearer node to the sink and it is the longest time undetected node
8: Send packet P_{kt} to node b
9: End for
10: for a detection packet received by each node (i.e. for node b) do
11: let $P_{kt}.\mu = P_{kt}.\mu - 1$, $P_{kt}.\overline{\mu} = P_{kt}.\overline{\mu} - 1$
12: if $\overline{\mu} = 0$ then
13: do value assignment for each part followed by the construction of feed_back packet fP_{kt}
14: send fP_{kt} to the source node
15: End if
16: if $P_{kt}.\mu \neq 0$ then
17: continue detection routing
18: End if
19: End for
20: for a feed_back packet fP_{kt} received by each node (i.e. for node c), do
21: if $fP_{kt}.destination$ is not itself then
22: send fP_{kt} to the source node
23: End if
24: End for

Packet-head	Packet-type	Source-ID	$\overline{\mu}$	μ	Packet-ID

Fig. 3 The structure of multi-detection route packets

Packet-head	Packet-type	Source-ID	Destination	Detection packet-ID	Packet-ID

Fig. 4 The structure of feed_back packets of a multi-detection route

- If $\bar{\mu} \neq 0$, then repeat the same process to choose the next hop in the same manner or else end the route.

In Fig. 4, the structure of a feed_back packet is depicted and it comprised with six essential parts namely, (i) Packet-head, (ii) Packet-type, (iii) Source-ID, (iv) destination node, (v) Detection packet-ID, and (vi) Packet-ID. The feedback packet is routed back to the data source; because nodes cache the detection route information and the feedback packet is able to return back to the source node.

4.3 Data-Routing Protocol

The process of routing nodal data to the sink is commonly referred as data-routing and the routing protocol seems similar to the commonly used MANET routing protocols [12, 13, 52, 56]. The major difference with the data-routing protocol and the existing MANET routing protocols (especially, on-demand routing protocols such as, AODV, AOMDV etc.) is that it improves the success ratio of the data packets reaching the sink; which means, the route will select a node with high trust for the next hop to avoid black holes.

In Fig. 2, the data-routing is shown using the pink arrow. As an example, we considered the shortest-routing protocol because; the data-routing protocol adopts the features of an existing routing protocol [35]. The neighbor node (i.e. node b) nearer to the sink and with high trust is selected by the source node a for considering this selected neighbor node as the next hop. In case, of the absence of a node with trust more than the default threshold value among all neighbor nodes closer to the sink, then it informs to the upper node that there is no path from source node a to the sink. Also, in the same way, the upper node continues its execution and will re-select a different node (i.e. node c) from among

Table 3 Pseudo-code of data-routing protocol

```
for a data packet created or received by each node (i.e. for node a ), do
select node b as the next hop and ensure that node b is an unselected node in
    the routing process and also possessing higher trust nearer to the sink
    if node a identifies such high trust node (e.g. node b )
     send P_kt (data packet) to node b
    if node b is the sink node then
      Accomplish this data routing process
    else
    Continue the data routing process with node b, such that node b has never
    been selected in this data routing process, has the largest trust and is nearer
    the sink
    end if
    else
      send feed_back failure to the node c , for instance, considered as upper node
    end if
end for
for the feed_back failure received by each node (i.e. for node b ), do
Repeat steps from 2 to 11
End for
```

its neighbors nearer the sink until the data are routed to the sink or there is conclusively no path to the sink.

4.4 Illustration of Data-Routing Protocol

In this, we detailed the implementation of the data-routing protocol. Table 3 illustrates the algorithm of data-routing protocol.

The major functionality of data-routing protocol is that whenever a data packet is received by any one of the node, the data-routing protocol choose a high trust node from the set of candidates nearer to the sink. It should be noted that, the selected node should possess higher trust than the predefined threshold value as the next hop. In case, the node fails to identify such kind of suitable next hop node, it will transmit a feed_back failure to the upper node. The upper node, in turn, re-computes the unselected node set and selects the node with the largest trust as the next hop. In the same way, the feed_back failure is transmitted to the upper node, if it fails to identify any such suitable next hop node.

4.5 Estimation of Nodal Trust

Nodal trust computation is performed by every node at the time of detection and data routing to co-operate for the avoidance of BHs (Black Holes). More considerably, at time T_j if node a performs a detection route for node b and ensuring that all the detection data are routed successfully, then assume $\nabla_a^b(T_j)$ be the trust of node a to node b or else consider $\Delta_a^b(T_j)$ be the trust. Considering that, the node a have Z interaction's with node b during time (T_j), the detection value order by time is as follows:

$\left\{\nabla_a^b(T_1)|\Delta_a^b(T_1), \nabla_a^b(T_2)|\Delta_a^b(T_2), \ldots \nabla_a^b(T_Z)|\Delta_a^b(T_Z)\right\}$, whereas, the trust value of node a to node b at time (T_j) is termed as $\nabla_a^b(T_j)|\Delta_a^b(T_j)$ and if data are dropped then, $\Delta_a^b(T_j) < 0$; otherwise $\nabla_a^b(T_j) > 0$).

4.5.1 Trust of Nodal Direction

Let us consider the trust set of node a and node b at the instance of time T as: $\left\{\nabla_a^b(T_1)|\Delta_a^b(T_1), \nabla_a^b(T_2)|\Delta_a^b(T_2), \ldots \nabla_a^b(T_Z)|\Delta_a^b(T_Z)\right\}$. Then, during time T, the total trust of nodal direction (i.e. from node a to node b) is defined as,

$$\begin{cases} c_a^b = \sum_{j=1}^{Z} \{(\nabla_a^b(T_j)|\Delta_a^b(T_j)) * \hat{w}(j)\}/Z, & Z \neq 0 \\ 0, & Z = 0 \end{cases} \tag{6}$$

However, with interactions $Z \neq 0$ the total direction trust of node a to b can be computed and if there is no interactions among node a and b (i.e.$Z = 0$), then it is impossible to compute the total trust between the nodes (because, there exists no path between the source node and the neighbor node having high trust than the predefined threshold value and which is nearer to the sink). In Eq. (6), $\hat{w}(j) \in [0, 1]$ represents an attenuation function for weighing nodal direction trusts at different times. Moreover, for the latest behavior it is essential to employ huge weight and otherwise employ minimum weight [51]. In Eq. (7), the attenuation function is derived; whereas, the parameter β represents a decimal less than one (i.e. $\beta < 1$).

$$\hat{w}(j) = \begin{cases} 1, & j = Z \\ \hat{w}(j-1) = \beta(\hat{w}(j), & 1 \le j < Z \end{cases} \tag{7}$$

In our proposed TEAR mechanism, it is necessary to meet some crucial conditions during trust computation. In the latest route detection, if a node is identified as legitimate or malevolent then its trust value should lie lower than the default threshold value $\mathfrak{R}$ and also that particular node will not be selected for later routing. In addition to this, if a malicious node wishes to return as an ordinary (normal) node, then that node requires several detections to enter into normal routing. Therefore, to compensate this criterion the parameter β should convince the following equation, they are as follows: For instance, assume the trust computation with Z communications (interactions) and the threshold is $\mathfrak{R}$, at the present situation the parameter β is responsible to satisfy the following condition:

$$((1-\beta^Z)/(1-\beta)-1) * \nabla_a^b < \mathfrak{R} - \Delta_a^b \tag{8}$$

For instance, if a node is shown to be malicious node, then we can obtain the criteria $\Delta_a^b(T_j) < 0$. But in case of the former $Z-1$ route detections, if the node is recognized as a trustable node, then the nodal trust (i.e. the trust of a node a to node b) should satisfy the formula as follows:

$\Delta_a^b + \beta\nabla_a^b + \beta^2\nabla_a^b + \cdots + \beta^{Z-1}\nabla_a^b < \mathfrak{R} \Rightarrow ((1-\beta^Z)/(1-\beta)-1) * \nabla_a^b < \mathfrak{R} - \Delta_a^b$, if there is more than one malicious node in the previous $Z-1$ route detections, the trust should be less than the threshold $\mathfrak{R}$.

The above said instance states that, if the malicious node wishes to return back to a normal node then there should be at least ψ trustable detections. Also, this node can be re-considered again as a trustable node. Therefore, the ψ trustable detections (ψ) should satisfy the following:

$$1 + \beta + \cdots \beta^{\psi-1} + \beta^{\psi}\partial + \beta^{\psi+1} + \cdots + \beta^{Z-1} > \mathfrak{R}/\nabla_a^b \tag{9}$$

4.5.2 Trust of Nodal Recommendation

Assume that, node a as the trust evaluator, the evaluation target is the node c and the recommender of node a is node b; hence, the trust direction from node a to node b is termed as c_a^b and the trust direction from node b to node c is termed as c_b^c; then from node a to node c the trust recommendation is determined as follows:

$$R_a^c = c_a^b \times c_b^c \tag{10}$$

The computation of multiple trust recommendations, that is from node a to b, b to c, etc.… till d to e be as follows:

$$R_a^e = c_a^b \times c_b^c * c_c^d \times c_d^e \tag{11}$$

4.5.3 Merging Trust Recommendation

Consider R_a be the recommender of node a such that,$m_j \in R_a$ and the trust recommendation from m_j to node k is termed as $R_a^{j,k}$; therefore, from node a to node k, the trust merge is estimated as follows:

$$V_a^k = \sum_{m_j \in a_n} \left(v_{m_j} R_a^{m_j,K} \right) \Big| v_{m_j} = \frac{R_a^{m_j,K}}{\left(R_a^{m_1,K} + R_a^{m_2,K} + \cdots + R_a^{m_{n-1},K} + R_a^{m_n,K} \right)} \tag{12}$$

4.5.4 Comprehensive Trust

The total trust is otherwise termed as comprehensive trust where, the trust direction and the trust recommendation are merged as follows:

$$C^{t}_{a,b} = \lambda C^{b}_{a} + (1 - \lambda) V^{b}_{a} \tag{13}$$

The total trust of a node is estimated by the following procedure: For each received feed_back packet the trust direction is estimated based on Eq. (6). This is done only after launching a detection route by the node. According to Eq. (10), the node interacts with the neighbors to obtain the trust recommendation. Then for multiple trust recommendations, the merge trust is computed based on Eq. (12). At last, the total trust (comprehensive trust) is computed based on Eq. (13).

4.6 Number of Dynamic Multi-detection Routes

Initially, we analyze the energy consumption at different distances from the sink. Let us assume that, r be the radius of the network, transmission radius among the nodes be R and the rate of event creation to be δ. In order to compute the nodal distance from the sink, the shortest routing protocol is employed [35, 36]. Hence, the nodal distance from the sink node ℓ is computed as $\ell = Nr + X$. The total number of data packets possessed by this node is shown below:

$$D_{\ell} = ((q + 1) + (q(1 + q)R)/2\ell)\delta \tag{14}$$

whereas q is an integer that converts $\ell + qR$ smaller than r and depending upon the total number of used data, the energy consumption can be inferred according to Eq. (14). Therefore, to symbolize the nodal load in this work, we consider the total amount of nodal data. This is due to the fact that, the lifespan of the network depends on the node that has the highest energy consumption. We consider, $D_{\max}$ as the maximum data load of the node (i.e. nodal data) and $D_{\max}E_v$ as the energy consumption. Moreover, we observed that if the data load in a node is lesser than $D_{\max}$, then that node still has the residual energy and this residual energy can be used to generate number of detection (multi-detection) routes. For instance, ℓ is the distance of a node to the sink and the residual energy of the node is $(D_{\max} - D_{\ell})E_v$, then this residual energy can be effectively used for detection. In case, hops are used to measure the distance of a dynamic detection route, then the possible nodal hops of the dynamic multi-detection route are determined as follows:

The maximum number of detection hops that can be attained by the remaining energy of nodes is with the nodal distance to the sink ℓ is:

$$\lambda_{\ell} = ((D_{\max} - D_{\ell})(1 + \eta_2))/(1 + \eta_2/\eta_1), \tag{15}$$

Hence, the ratio between the detection packet-length to the data packet length is represented as η_1 and the ratio between head packet length to the data packet length is denoted as η_2, respectively.

Figures 5 and 6 delineate the maximum number of detection hops obtained with the remaining nodal energy (i.e. residual energy) with different distances of the node from the sink. It should be noted that, in non-hotspots the residual energy is in higher level because, it possess small detection packet length. If the radius of the network (i.e.$r = 500$ m), then the detection hops can be counted in hundreds. From this fact, it

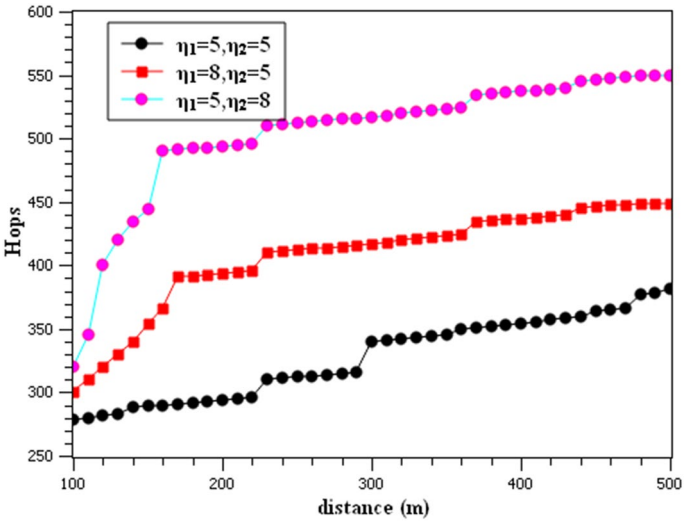

Fig. 5 Number of detection hops provided by the residual energy of the nodes (various η_1, η_2)

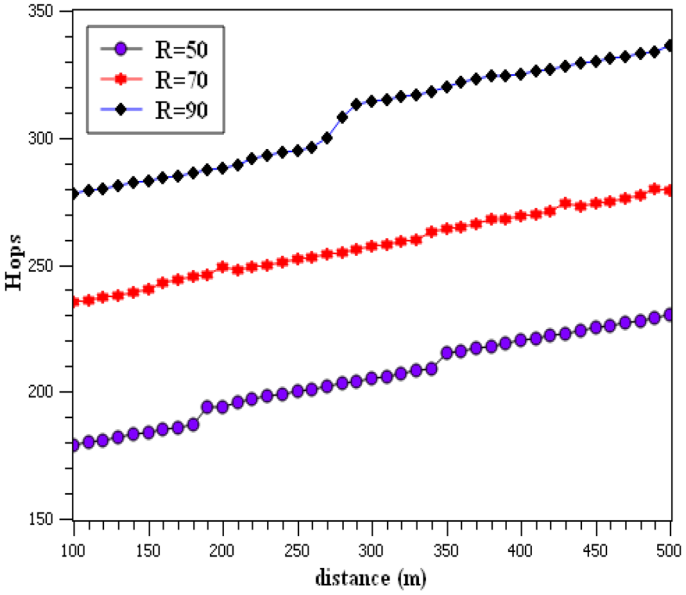

Fig. 6 Number of detection hops provided by the residual energy of the nodes (various R)

is observed that the network holds enough energy for further processing the detection routes without troubling the lifespan of the network.

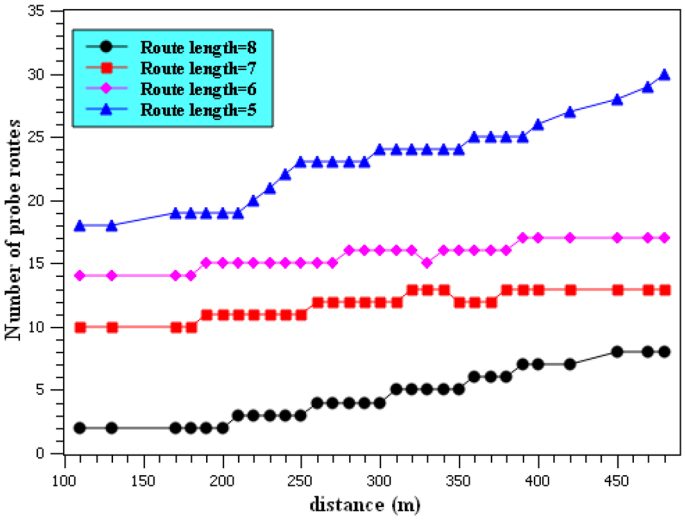

Fig. 7 Number of probing routes that can be generated by varying the distance from sink

Proposition 1 *The TEAR mechanism has the same network lifespan as the mechanisms not considering any security strategy.*

Proof In order to create multi-detection routes our TEAR mechanism uses the remaining energy of the node. This effective process will not make the nodal energy consumption to exceed beyond $D_{\max}$, therefore, the lifetime of the network still remains $\phi = \frac{e_{init}}{D_{\max}}$.

Figure 7 delineates the probe route generation with remaining energy of the non-hotspots in a network with radius $r = 500$ m.The probe routes are generated using the remaining energy in non-hotspots under the detection route lengths of 5–8. We observed that, for about seven detection routes, the residual energy can provide full support.

4.7 Analyzing the Probability of Successful Routing

Let us assume that, n_d be the nodal degree and y be the length of the detection route (i.e. number of hops) determined after single round. Moreover, the term M_{in} is the nodes with least in-direction trust, M_d be the nodes that possess the direction trust, and M_{on} be the nodes that fail to obtain the trust. It is determined as follows:

$$M_d = (1 - 1 - \phi)^y)/\phi,\ M_{in} = (1-p)n_d,\ M_{on} = (n_d - M_d)p | M < n_d \tag{16}$$

whereas,

$$\begin{cases} p = 0 & if\ \beta < 2u | \beta = (1 - \frac{\sqrt{3}}{2\times\pi})n_d - 2 \\ p = \frac{(\beta-u)!(\beta-u)!}{\beta!(\beta-2u)!} & if\ \beta \geq 2u | u = \frac{\left((1-\frac{\sqrt{3}}{2\times\pi})n_d - 2\right)M_d}{n_d} \end{cases}$$

In order to compute the average length of the route, consider the ratio of the malicious node as ϕ, y be the number of hops (the detection route length), the routing may accomplished earlier due to the entrance of a BH (Black Hole). The actual average route length for the route length y is computed as follows.

The probability of BH (Black Hole) detection at the first event is denoted as ϕ, and $(1-\phi)\phi$ is the probability of not detecting the BH even though at the second event; hence, the probability of not detecting the BH even though at j^{th} event is termed as $(1-\phi)^{j-1}\phi$.

Therefore, the actual average 'route length' is expressed as follows:

$$M_d = \phi + 2(1-\phi)\phi + \cdots + j(1-\phi)^{j-1}\phi + \cdots + y(1-\phi)^{y-1}\phi \tag{17}$$

Moreover, the Eq. (18) can be simplified into $M_d = (1-(1-\phi)^y/\phi$. This can be performed after complex processing. Considerably, with length y if each node executes a single round of detection and then by evaluating the average, we observed that it can be applied for each node to execute detection routes M_d to its neighbors. Therefore, M_d be the direction trust for the number of nodes.

Figure 8 depicts the in-direction trust among the nodes. Whereas, the node a and node b possess least amount of common neighbors and the probability of in-direction trust is lower among these nodes. It can be computed as follows:

More significantly, the most common nodes identified in nodes a and b are recognized as the number of nodes which are employed in the equivalent transmission radius. Also, for this region the area is computed as $2\left(\Pi R^2/3 - \frac{\sqrt{3}}{2} \times \frac{1}{2}R^2\right) = \frac{2}{3}\Pi \times R^2 - \frac{\sqrt{3}}{2}R^2$. Thus, the total number of nodes embedded in this region is $\left(\frac{2}{3}\Pi R^2 - \frac{\sqrt{3}}{2}R^2\right)\sigma = \left(\frac{2}{3}\Pi R^2 - \frac{\sqrt{3}}{2}R^2\right)n_d \Big/ \Pi \times R^2$. The total number of general neighbors, except from node a and b is $\beta = \left(\frac{2}{3} - \frac{\sqrt{3}}{2\times\Pi}\right)n_d - 2$. Then for the general (common) neighbors the total number of detections is estimated after processing M_d detections by a node a, which is shown below:

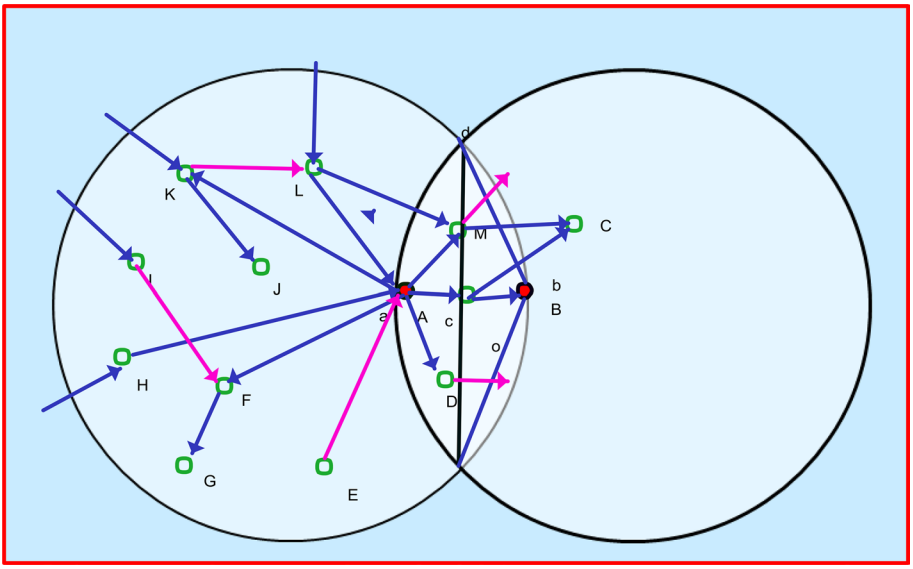

Fig. 8 In-direction trust between the nodes

$$u = \frac{\left((\frac{2}{3} - \frac{\sqrt{3}}{2\times\Pi})n_d - 2\right)M_d}{n_d} \tag{18}$$

Hence, the Eq. (19) can also be effectively applied to node b. The probabilities are more dissimilar for these two groups and they are depicted below:

$$\begin{cases} P = 0 & if \quad \beta < 2u \\ P = \frac{C_{\beta}^{u} \times C_{\beta-u}^{u}}{C_{\beta}^{u} \times C_{\beta}^{u}} = \frac{(\beta-u)!(\beta-u)!}{\beta!(\beta-2u)!} & if \quad \beta \geq 2u \end{cases} \tag{19}$$

Therefore, P be the probability that the node a fails to acquire the in-direction trust of node b. Notably, the node a possesses n_d neighbors and between this they include M_d nodes which have the ability to hold the direction trust, the nodes (i.e. $M_{in} = (1-p)n_d$ that holds the in-direction trust and the nodes that fail to hold trust is referred to as $M_{on} = (n_d - M_d)p | M < n_d$.

Proposition 1 *Consider the trust direction and the total number of trust direction nodes represented as M_d, then the "success rate" determined for the data packets transmitted by the nodes to the sink which are away from κ hops is as follows:*

$$\begin{array}{ll} \gamma_d^{\kappa} = (1 - \phi^{n_d/3})^{\kappa-1} & if \quad M_d \geq n_d \\ \gamma_d^{\kappa} = (1 - \phi^{M_d/3+1})^{\kappa-1} & if \quad M_d < n_d \end{array} \tag{20}$$

Proof Initially, determine the node *a's* success rate for 1-hop transmissions. In case, a transmission is failed then we can recognize that node a identifies entire detected nodes (i.e. whose hops are smaller than itself are BHs). After identifying the black holes, these detected nodes were ignored; hence the node a made an attempt to choose from the undetected nodes. Conversely, the chosen unnoticed (undetected) node is also a BH, and then the transmission is discontinued. Therefore the probability of failure is computed as follows:

The node a is comprised with 3 hop stages such as, larger hop nodes than node a, same hop nodes more similar to node a and smaller hop nodes than node a. The smaller hop nodes than the hop counts of node a with the nodal degree n_d is termed as $n_d/3$. Thus, these smaller hop nodes include $M_d/3$ detections along the total of M_d'detections'. The neighbors that relates to node a can be exactly identified in the criterion $M_d \geq n_d$ and the transmission failure may occur only in the condition if all of the subsequent 'hop nodes' are malicious (i.e. especially black nodes). The probability for these criterions can be computed as:

$\chi_1 = \phi^{n_d/3}$. Appropriately, the probability of black node for each 'detection' represented as $\phi^{M_d/3}$ is determined at the condition $M_d < n_d$. Also at this condition, while selecting the next hops the probability of black node is termed as $\phi^{M_d/3+1}$. Therefore, the probability of transmission failure is computed as $\chi_1 = \phi^{n_d/3+1}$.

Therefore, for a node present at the k-hops from the sink, if data are sent k-hops and to the last hop is not recognized as a malicious node (i.e. black node), then for each hop the probability of successful transmission is,

$$\begin{array}{ll} \gamma_d^{\kappa} = (1 - \phi^{n_d/3})^{\kappa-1} & if \quad M_d \geq n_d \\ \gamma_d^{\kappa} = (1 - \phi^{M_d/3+1})^{\kappa-1} & if \quad M_d < n_d \end{array}$$

thus proved.

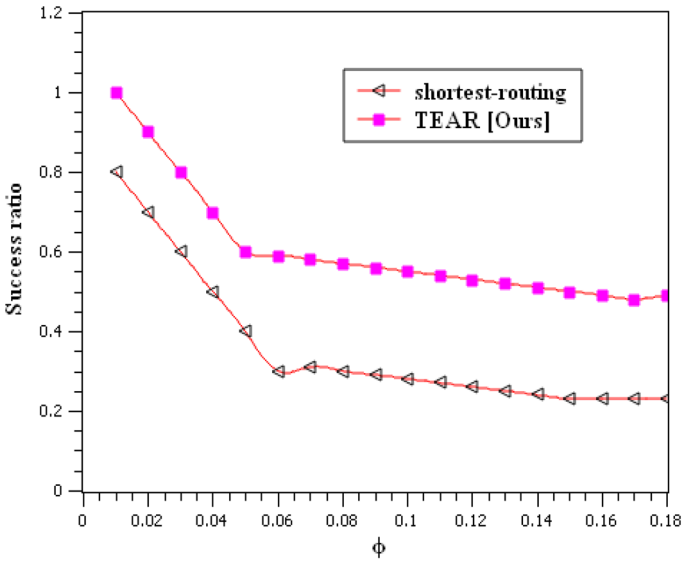

Fig. 9 Probability of success ratio

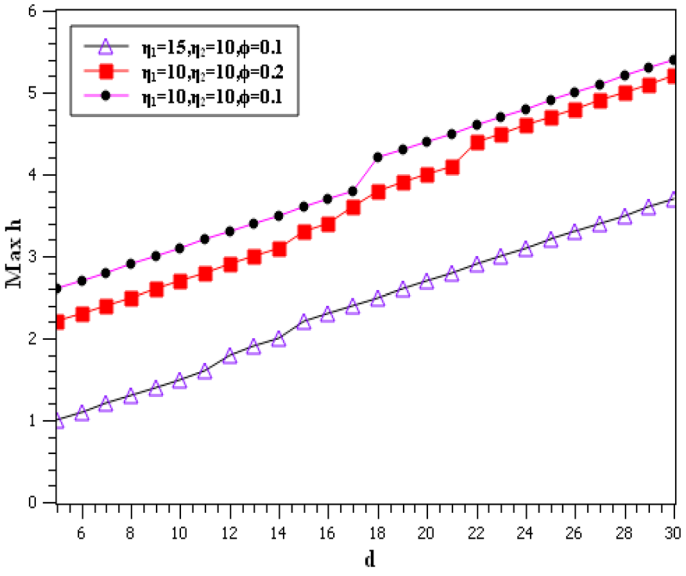

Fig. 10 Network scale that makes the nodal degree lower than the number of detected nodes without degrading the lifespan of the network

Figure 9 depicts the total success rate obtained for a data route with our TEAR mechanism if only one detection route length $\mu = 5$ is used. Moreover, when compared with the shortest routing mechanism [35, 36] our proposed TEAR mechanism achieves higher probability of total success ratio. From Fig. 10, we inferred that in a nodal-degree of 30

and the networks scales employed is only 7-hops, then the residual energy that relays on the non-hotspots region acquires the ability to execute more number of detection routes even though in a single data collection round. This process is done to detect the trust of all neighbors without degrading the lifespan of the network. Also, we inferred that better security is obtained throughout the entire lifespan of the network.

From Fig. 10, we inferred that in a nodal-degree of 30 and the networks scales employed is only 7-hops, then the residual energy that relays on the non-hotspots region acquires the ability to execute more number of detection routes even though in a single data collection round. This process is done to detect the trust of all neighbors without degrading the lifespan of the network. Also, we inferred that better security is obtained throughout the entire lifespan of the network.

According to Proposition 1, if the number of direction detection nodes is larger than the nodal degree, which means that all neighbors are detected and all neighbor trust is obtained, only a scenario in which all neighbors are black nodes can cause the transmission to fail. By chance, if this condition emerges, then none of the mechanism can solve this problem because all paths to the sink are blocked by black nodes. Therefore, the situation in which the number of detected nodes equals the nodal degree is optimal. In the following proposition (theorem 2), we analyze whether this ideal situation can be achieved in MANETs.

Proposition 2 *The success ratio of our mechanism when nodes those are κ-hops away from the sink and after adopting the shortest route, we obtained the following:*

$$\alpha_{\kappa} = \gamma_d^{\kappa} / (1-\phi)^{\kappa}(1-\phi)^{\kappa} \tag{21}$$

Proof The ratio of the black node in the network (ϕ) and nodes that are κ-hops away from the sink due to the random selection of nodes, the probability of a black node in the network (ϕ) is same as the black node ratio in the network. The last hop is not being

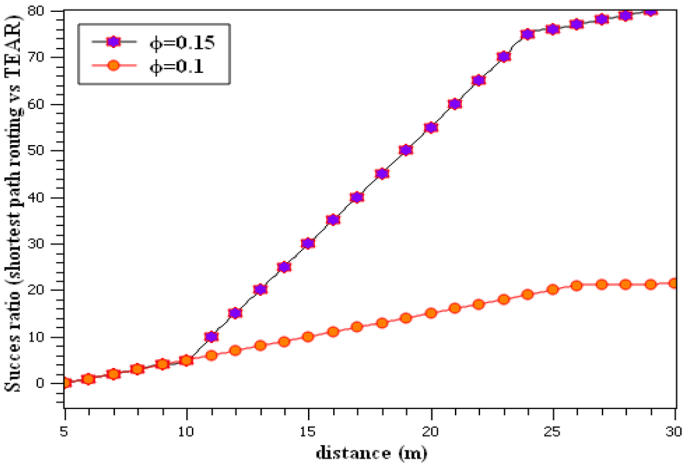

Fig. 11 Probability of success ratio with TEAR mechanism to the shortest-routing mechanism

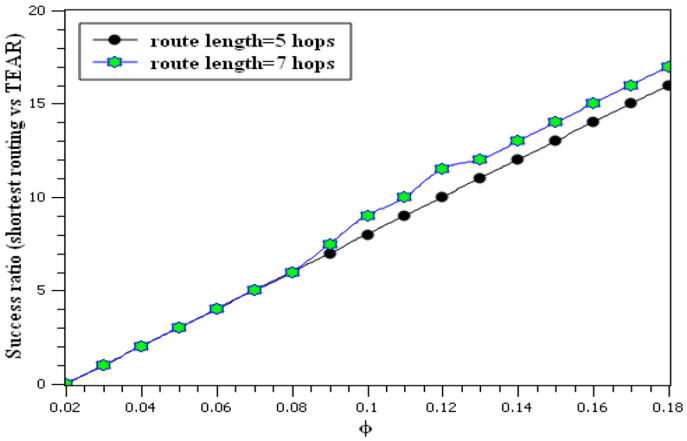

Fig. 12 Total probability of success ratio with TEAR mechanism to the shortest-routing mechanism

recognized as a black node; thus, with the shortest-route mechanism, the probability of all the non-black nodes chosen subsequent to κ-hops is $(1-\phi)^{\kappa-1}$, and the ratio of TEAR mechanism to the shortest-route scheme [36] is determined as $\alpha_{\kappa} = \gamma_d^{\kappa} / (1-\phi)^{\kappa}(1-\phi)^{\kappa}$, hence proved.

From Figs. 11 and 12, we analyzed the enhanced performance of our proposed TEAR mechanism to the shortest-path mechanism. From this, we can infer that, as the distance from the sink increases, more hops are required for data to be transmitted to the sink, so the success ratio in the shortest route scheme is low; however, our TEAR mechanism is based on the detected nodal trust, and the success probability is higher because of the selection of high trust nodes. If the black node ratio is higher, it is more improved by our TEAR mechanism (up to 10 times more), thus proving the effectiveness of our mechanism.

Table 4 Simulation parameters

Parameter	Values
Simulation time	800 s
Simulator	NS2
Simulation area	1000 × 1000 m
Mobility model	Random way point
Number of nodes	1000 nodes
Data packet size	512 byte
Bandwidth	2 Mb/s
Radio range	245 m

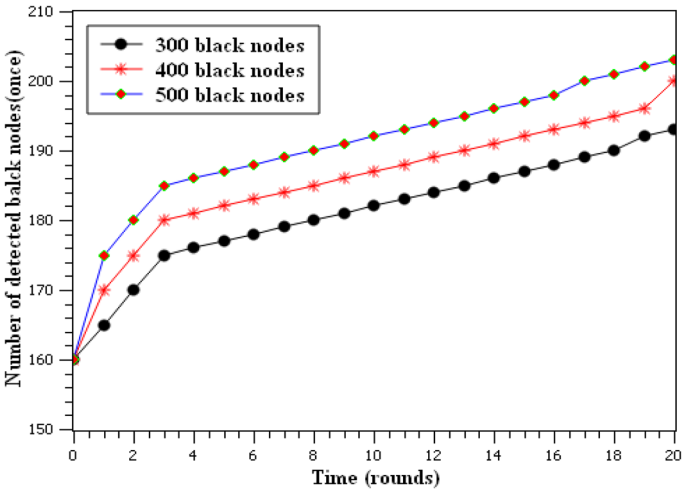

Fig. 13 Number of black nodes detected with various network runs

5 Experimental Analysis

The experimental analysis is done in the NS2 platform. To evaluate the performance of the proposed mechanism, experiments were conducted by deploying 1000 nodes in the network. About 300 nodes deployed are black nodes and the nodal speed ranges about 0–15 m/s employing the RandomWay point mobility model [57–59]. The nodes are distributed randomly in a 1000×1000 m field and the simulation time employed is 800 s. Table 4 depicts the simulation parameters.

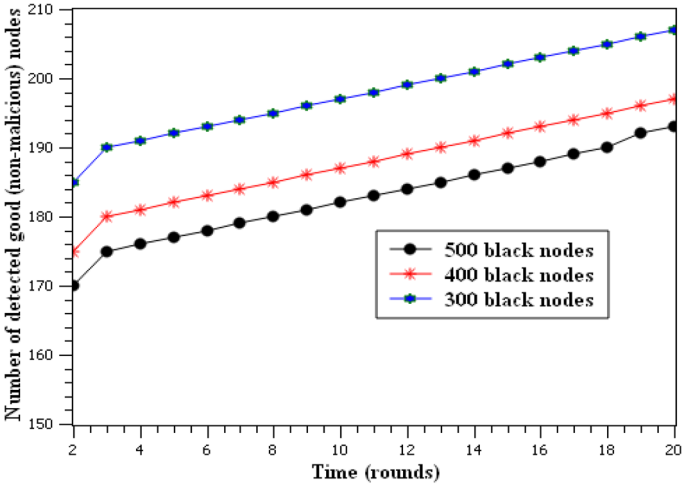

Fig. 14 Number of non-malicious nodes detected with various network runs

5.1 Experimental Analysis of Nodal Trust

From Fig. 13, we analyzed the efficiency of our proposed TEAR mechanism in the detection black nodes that interrupts the data transmission. For each and every round of data collection, a single detection route with a length 5 is initiated by each node. After certain runs (i.e. as multi-detection routes are performed), the quantity of detected black nodes increases rapidly in case black nodes which are deployed varies in the range of 300, 400, 500 and so on. The simulation time required to detect all the employed black nodes are 5, 8 and 12 rounds respectively. From this, we can ensure that our proposed TEAR mechanism requires only limited time and minimum detections to identify the malicious nodes. After employing the same experimental view of Figs. 13 in 14, we analyzed that our proposed TEAR mechanism only with 4 rounds all the non-malicious nodes are detected over the network runs. This is due to the fact that our proposed mechanism embedded the data-routing protocol and this protocol requires only a finest 'downstream' node to route the data to the next-hop. From this, we can ensure that our proposed mechanism can provide more flexible routing and generates high "success rate" probability.

Figure 15 shows the performance of our TEAR mechanism on the detection of black nodes with twice detection on each data collection rounds. When contrasted with single detection rather than twice detecting, the speed is doubly enhanced with twice detection of black nodes and with at most seven rounds all the black nodes are identified. The same problem is illustrated in Fig. 16, which ensure that after employing multi-detection routes (i.e. more detection routes) even though in single round of data collection all the black nodes are detected with minimum time consumption. This proves that our proposed TEAR mechanism enhances the network security by identifying all the black nodes quickly with multi-detection routes (i.e. black nodes can be more quickly detected as the detection grows). Also, the residual energy that relays in non-hotspots region can provide higher efficiency in the detection of black nodes which mean 7 times or more

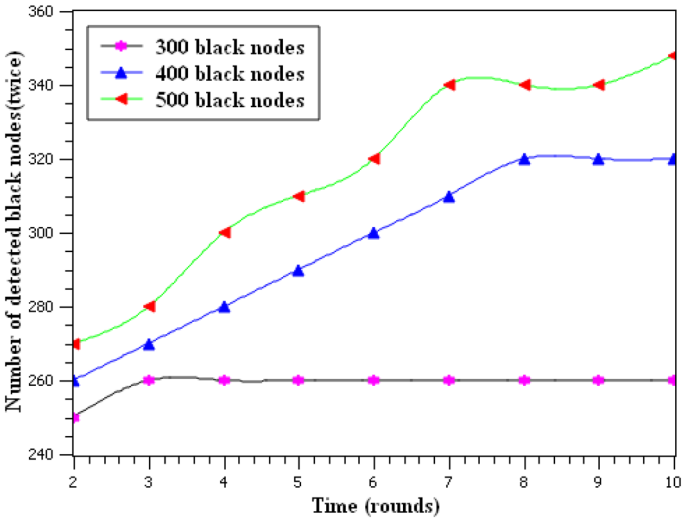

Fig. 15 Number of black nodes detected with various network runs

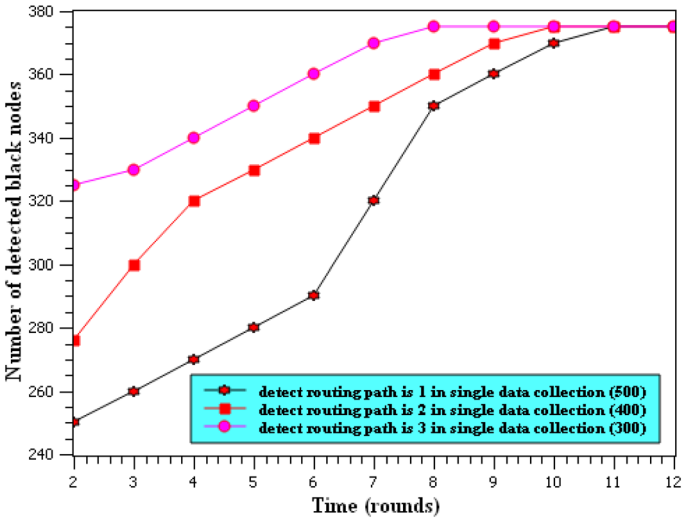

Fig. 16 Number of black nodes detected with single round of data collection over multiple 'detection' routes

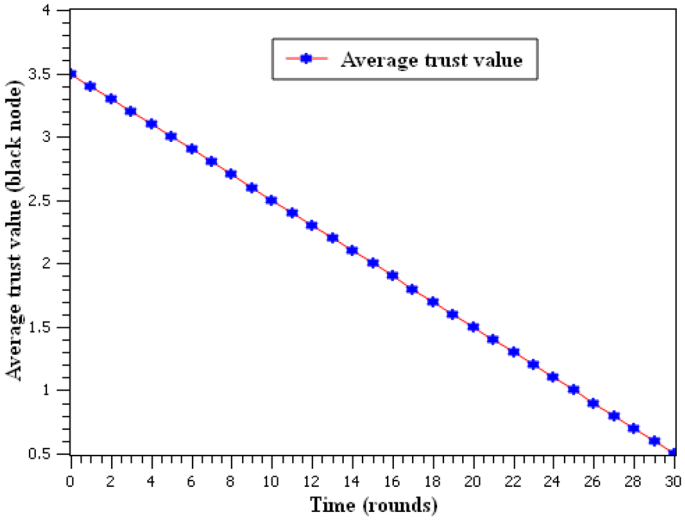

Fig. 17 Trust value of black nodes with the network runs

than 10 times efficiency. In other words, the residue energy in non-hotspots can afford 7 times (or even more than 10 times) detecting; if all of the residue energy is used to construct detection routes, the system can detect almost all of the black nodes in at most two data collection rounds, which fully verifies the fast recognition ability of our TEAR mechanism.

The experimental view of Figs. 17 and 18 is analyzed after deploying 400 black nodes of 1000 nodes in the network. Moreover, in each data collection round, each node

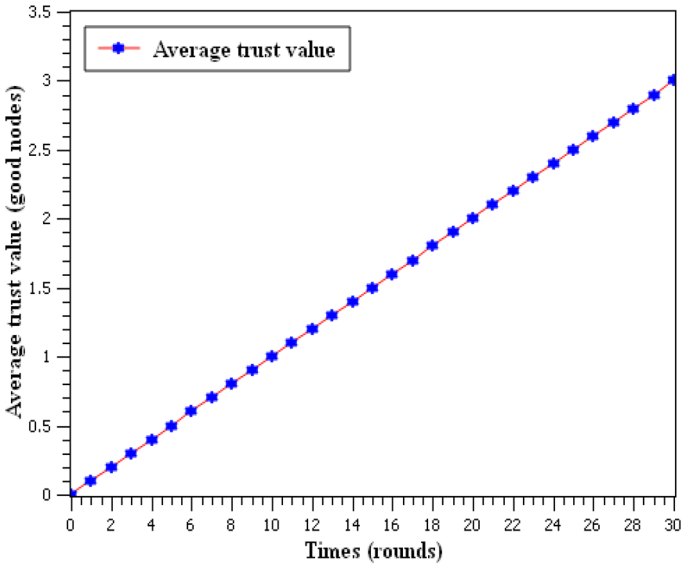

Fig. 18 Trust value of non-malicious nodes with the network runs

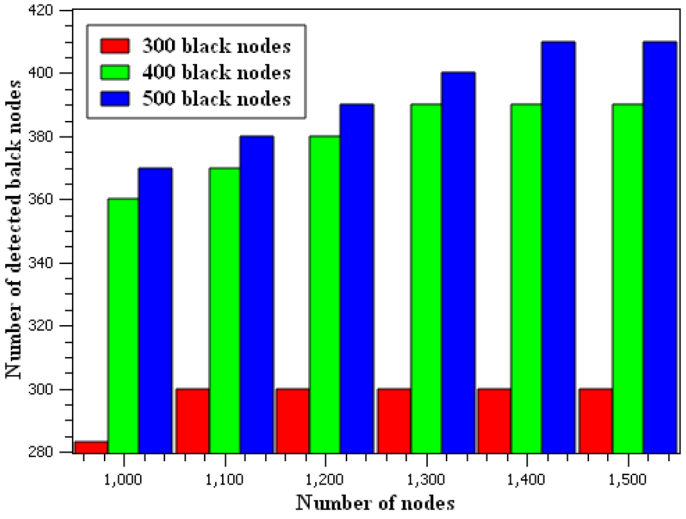

Fig. 19 Number of black nodes detected with different number of nodes

creates detection once. From Figs. 17 and 18, we observed that the average of black nodes trust decreases with each network runs whereas, the average of finest (good) nodes trust improves with each network runs.

Figures 19 and 20 depicts the number of black nodes and finest (good) nodes identified after two rounds of data collection when each node detects once in each round for a network of 1000–1500 nodes including black nodes (300, 400 and 500). Form Fig. 18, we can observe that when employed 300 black nodes, the nodal density is increased and

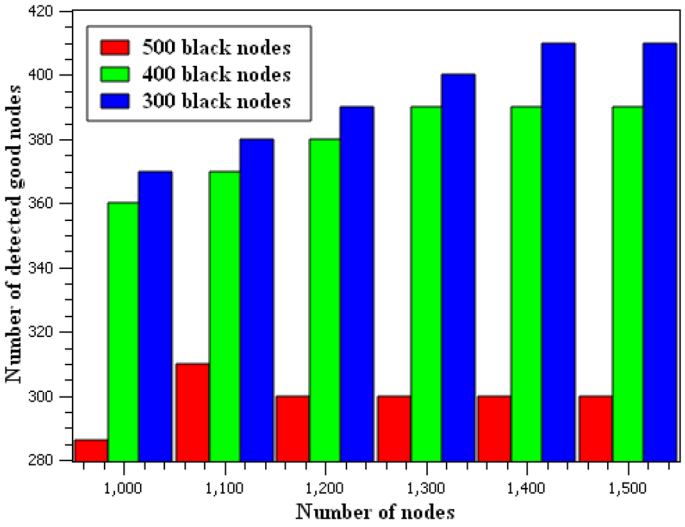

Fig. 20 Number of non-malicious nodes detected with different number of nodes

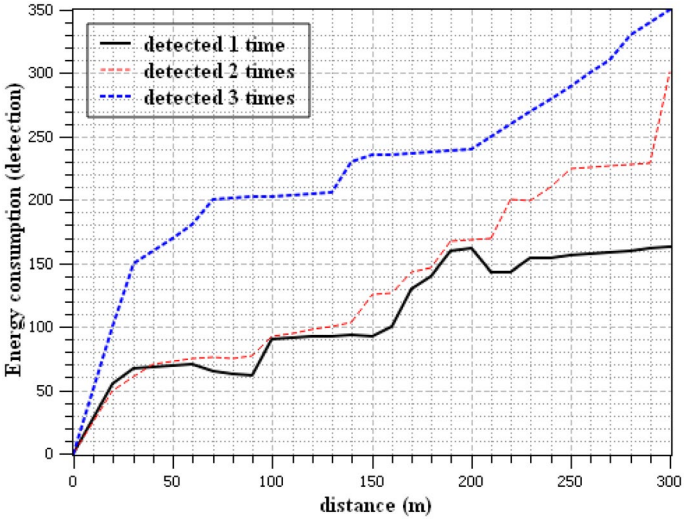

Fig. 21 Energy consumption required for detection at different sink distances

the possibility of detecting the black nodes is slightly limited. But, in case, if 500 black nodes are employed, the possibility of detecting the black nodes is highly improved with increased nodal density. This proves that our proposed TEAR mechanism can perform well with increased nodal density. From Fig. 19, we can infer that increased nodal density can provide further growth in the detection of non-malicious (good) nodes. The probability of successful routing is highly improved with increased nodal density in our proposed TEAR mechanism.

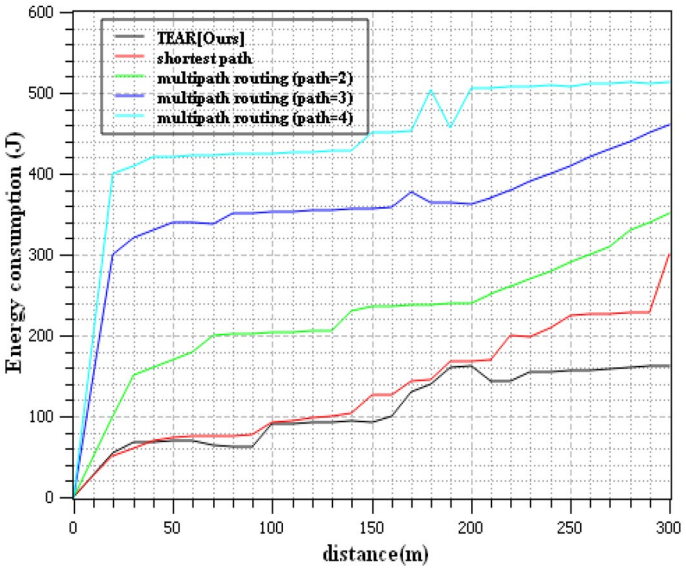

Fig. 22 Energy consumption over different routing mechanisms

5.2 Energy Consumption

From a single round of data collection, the energy intake of each node is detected three times within a radius $r = 500$ m and 1000 nodes are deployed. Moreover, among 1000 nodes there include 400 black nodes. Figure 21 depicts the detections of total energy consumption of nodes three times with the increase of nodal distance from the base station (sink). From the analysis, we inferred that the energy consumption among the nodes is equally shared, excluding the fact that the nodes that are closer to the sink consumes minimum energy with an end goal to minimize the energy consumption in 'hotspots'. When moving towards other regions the energy consumption of the nodes is balanced, but with the increase of detection routes, the energy consumption is increased.

Figure 22 depicts the energy consumption of nodes after a single round of data collection by varying the distance from the sink. From the analysis we inferred that the shortest-path routing mechanism [35, 36], consumes only minimum energy (as explained previously). When compared with the multi-path routing [33, 34] one data packet is sent to the sink via different paths to improve the success rate, more packets reach the sink, and the energy consumption is proportional to the number of paths, i.e., the more paths there are, the higher the energy consumption is and the higher the success rate is for data arriving at the sink. Although the success rate increases as the number of paths grows, there are some problems. (1) The success rate is not high; for instance, if the success rate for each path is 20%, then even if 10 paths are created, the success rate does not reach 90%. (2) Even if a certain success rate is achieved, the network lifetime is affected. Therefore, in our scheme, by constructing dynamic detection routes, malicious nodes can be detected without affecting the network lifetime, which also improves the success rate with good performance.

Figure 23 depicts the ratio of nodal energy consumption to the number of packets routed to the sink. We done the analysis by maintaining the same energy consumption to

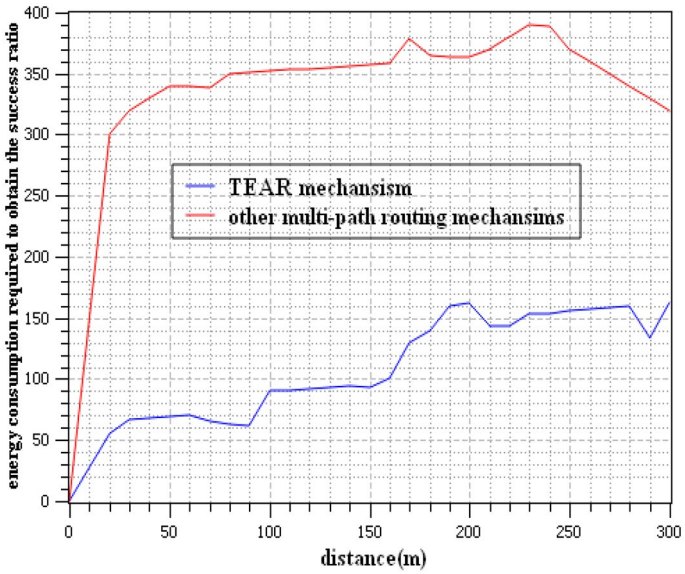

Fig. 23 Total energy consumption over different multi-path routing scenarios

the number of packets routed to the sink in different mechanisms. The network efficiency is analyzed with different mechanism. From the analysis, we inferred that our proposed TEAR mechanism achieves maximum energy efficiency (i.e. more than 2 times) as compared with the conventional routing mechanisms.

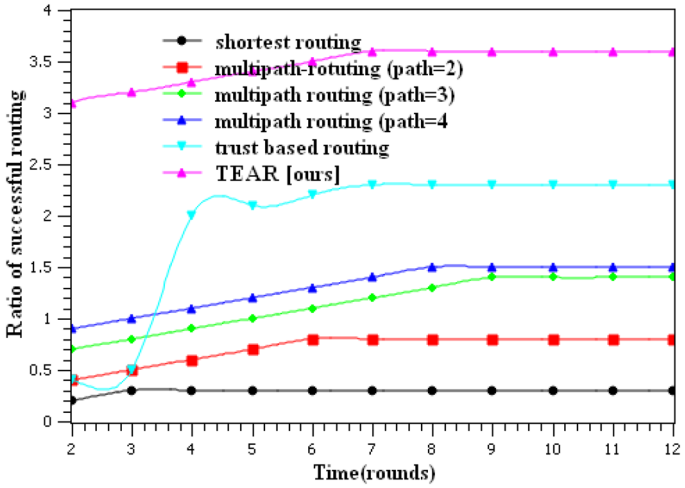

Fig. 24 Ratio of successful routing with the network runs

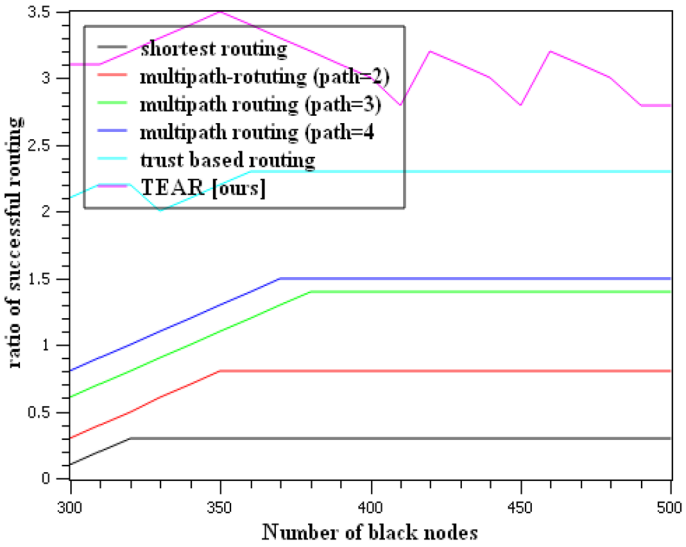

Fig. 25 Ratio of successful routing with different number of black nodes

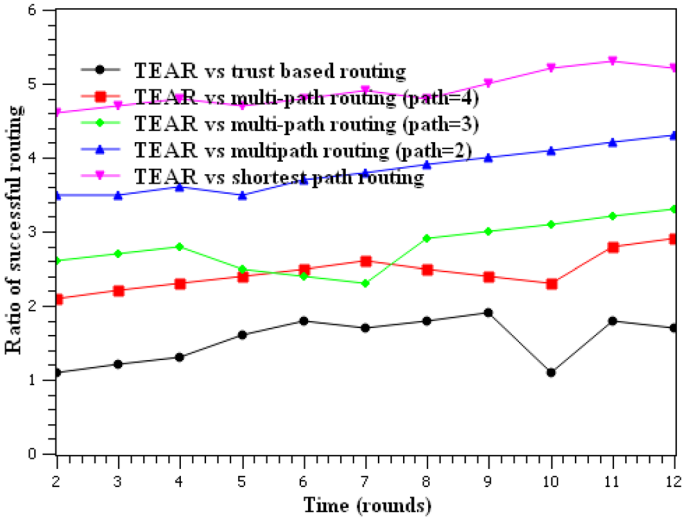

Fig. 26 Probability of 'successful routing with different network runs

5.3 Comparative Analysis with the Probability of Successful Routing

The probability of successful routing is analyzed by changing the runs of the networks to the rounds of data collection (i.e. about 7 rounds). Moreover, among 1000 nodes, 400 black nodes are included whereas a single detection is done by each node. After analysis, we inferred that, the shortest-routing mechanism achieves successful routing probability lesser than 15%. Hence, the multi-path routing after employing 4 paths achieves the probability

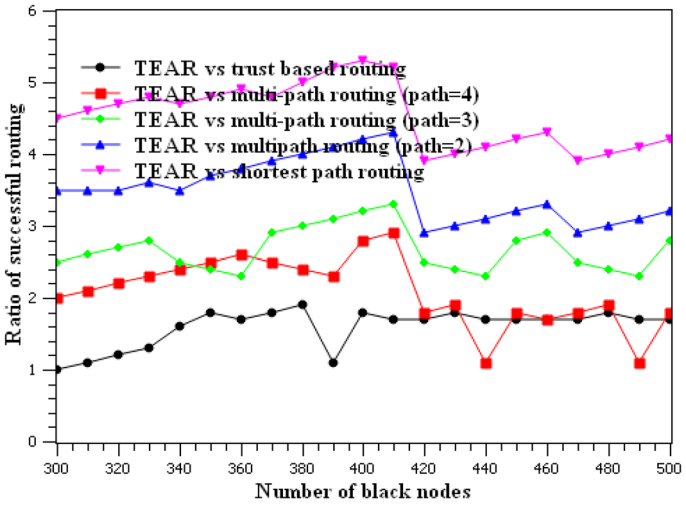

Fig. 27 Probability of successful routing with different number of black nodes

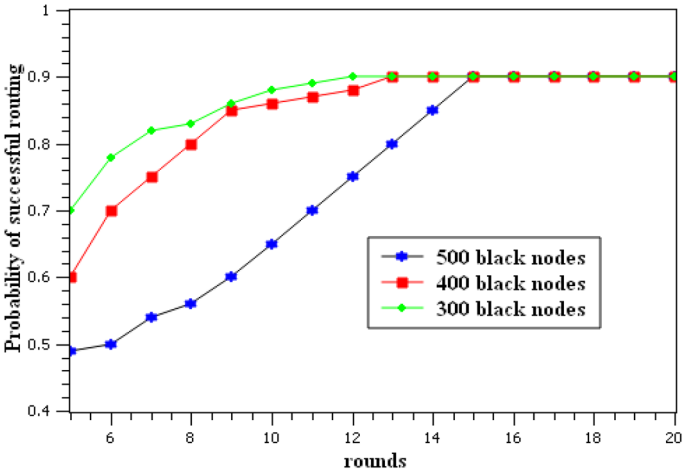

Fig. 28 Ratio of successful routing

of about 60%. Consequently, this 'black node' avoidance mechanism doesn't bother about the total runs of the network and there is no way in the improvement of the successful routing probability beyond this particular limit. The trust based routing mechanism [31, 32] is somewhat similar to our proposed mechanism, in which the mechanisms evaluate the trust value of nodes for the better selection of next hop for further routing. Therefore, with increase in time, the successful routing probability also increases (Fig. 24). However, the conventional routing mechanisms fail to detect the trust of nodes in active (dynamic) manner, therefore the probability of successful routing is minimum than our proposed TEAR mechanism. Moreover, the successful routing probability is compared by varying

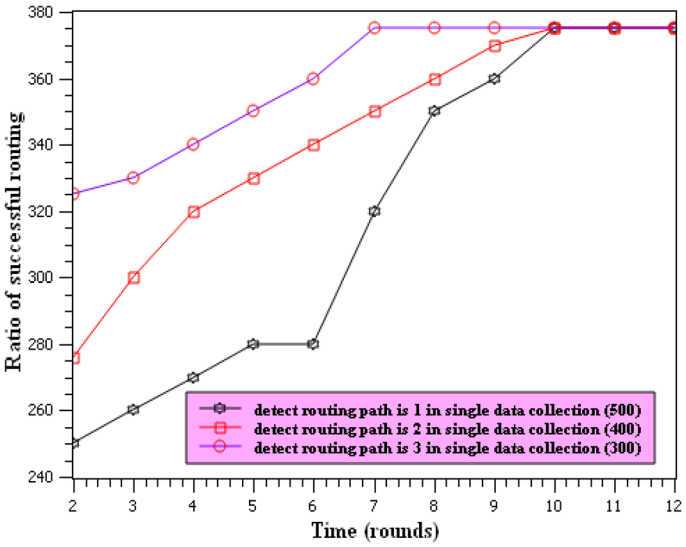

Fig. 29 Ratio of successful routing with single data collection round over different number of detection routes

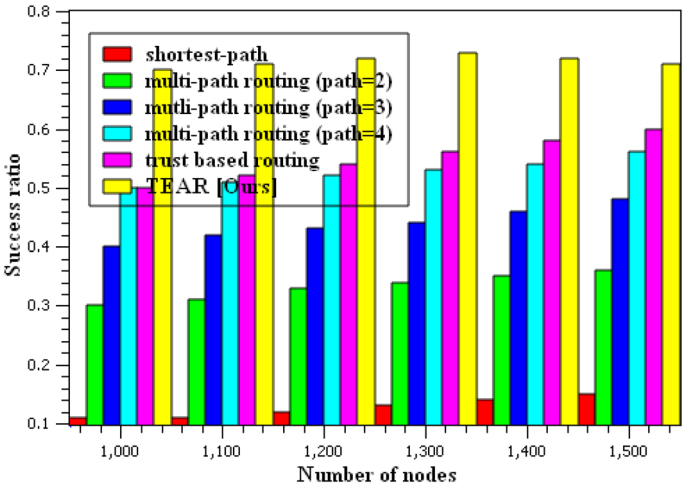

Fig. 30 Success ratio with different number of nodes

the number of black nodes (Fig. 25). Figure 26 depicts the improvement of our mechanism contrasted to other routing mechanism, from the analysis; we can infer that our proposed mechanism exhibits better performance than other conventional routing mechanisms. For a short period if the network runs, then the probability of successful routing is enhanced from 1.5 to 6 times. Moreover, comparison is done by varying the number of black nodes under different mechanism (Fig. 27). From the analysis, we inferred that our proposed TEAR mechanism exhibits better performance (i.e. more than 3 times) than the conventional multi-path routing, shortest-path routing and trust-based routing mechanism.

Figure 28 depicts the successful routing probability over TEAR mechanism with various network runs. From the analysis we inferred that, even though with single round of data collection and with single detection, the probability achieved is about 100%. Figure 29 illustrates depicts the successful routing probability over TEAR mechanism with single round of data collection and with 1, 2 and 3 detections. In view of the fact, we analyzed that if the detection routing path is three, then after only three rounds, our proposed TEAR mechanism achieves 100% probability. This proves that our proposed TEAR mechanism achieves higher successful routing probability.

Furthermore, we varied the number of nodes and analyzed the probability of successful routing for different schemes (Fig. 30). From the analysis, we inferred that the nodal degree exceeds with the growth of nodal density; hence it will increase the ratio of successful routing. The reason is that with the further growth of both the nodal density and nodal degree, then there are more detected trustable nodes after detection, that is, there are more nodes for the next hop, and the probability of successful routing thus increases. Moreover, we inferred that our proposed TEAR mechanism enumerates the positive effects on serious network threatening Black Hole Attacks (BHAs).

6 Conclusion

In this paper, we have proposed a novel Trust based Energy Aware Routing (TEAR) mechanism that works on the basis of dynamic multi-detection routing protocol. The excellent characteristics that relays on our proposed TEAR mechanism are as follows: (a) Increased scalability, security and increased probability of successful routing. In order to attain 100% ratio of successful routing probability, the TEAR mechanism provide maximum effort to avoid the malicious (suspicious) nodes quickly as possible by detecting the nodal trust. (b) Maximum energy efficiency. In order to construct the multiple detection routes, our TEAR mechanism completely utilized the residual energy. The theoretical and experimental analysis proved the efficiency of our proposed TEAR mechanism than other conventional routing mechanism (i.e. more than three times or 10 times in some rare cases). Moreover, our mechanism provides better network security and effective energy efficiency. For future work, we plan to evaluate dynamic blacklists by setting different values to certain variables on the basis of number of nodes and number of links among them to reduce the generated communication overhead to make it more scalable.

References

1. Camp, T., Boleng, J., & Davies, V. (2002). Survey of mobility models, wireless communication and mobile computing (WCMC). *Special Issue on Mobile Ad Hoc Networking: Research, Trends and Applications, 2*(5), 483–502.
2. Sundararaj, V. (2019). Optimal task assignment in mobile cloud computing by queue based ant-bee algorithm. *Wireless Personal Communications, 104*(1), 173–197.
3. Sundararaj, V., Muthukumar, S., & Kumar, R. S. (2018). An optimal cluster formation based energy efficient dynamic scheduling hybrid MAC protocol for heavy traffic load in wireless sensor networks. *Computers & Security, 77*, 277–288.
4. Singh, G., Bindra, H., & Sangal, A. (2011). Performance analysis of DSR, AODV routing protocols based on wormhole attack in mobile ad hoc network. *International Journal of Computer Applications, 26*(5), 38–41.

5. Irshad U., & Rehman S. U. (2010). Analysis of black hole attack on MANETs using different MANET routing protocols. Master thesis, School of Computing, Blekinge Institute of Technology, Sweden.
6. McMahon, R. (2004). *Introduction to networking*. New York: McGraw-Hill Higher Education.
7. Tseng C. (2006). Distributed intrusion detection models for mobile ad hoc networks. Ph.D. thesis, University Of California Davis.
8. Aljawarneh, S., Aldwairi, M., & Yasin, M. B. (2017). Anomaly-based intrusion detection system through feature selection analysis and building hybrid efficient model. *Journal of Computational Science, 25,* 52–160.
9. Aljawarneh, S., Yassein, M. B., & Telafeh, W. (2017). A resource-efficient encryption algorithm for multimedia big data. *Multimedia Tools and Applications, 76,* 1–22.
10. Aljawarneh, Shadi A., Moftah, Raja A., & Maatuk, Abdelsalam M. (2016). Investigations of automatic methods for detecting the polymorphic worms signatures. *Future Generation Computer Systems, 60,* 67–77.
11. Sundararaj, V. (2016). An efficient threshold prediction scheme for wavelet based ECG signal noise reduction using variable step size firefly algorithm. *International Journal of Intelligent Engineering and Systems, 9*(3), 117–126.
12. Johnan, D. B., & Maltz, D. A. (1996). Dynamic source routing in ad hoc wireless networks. In T. Lmielinski & H. Korth (Eds.), *Mobile computing, chapter 5* (pp. 153–181). Amsterdam: Kluwer Academic Publishers.
13. Perkins, C. E., & Royer, E. M. (1999) Ad hoc on-demand distance vector routing. In *Proceedings of the 2nd IEEE mobile computer systems and applications* (pp. 90–100).
14. Lee, S. J., & Gerla, M. (2011). Split multipath routing with maximally disjoint paths in ad hoc networks. In *IEEE ICC* (pp. 3201–3205).
15. Kanthe, A., Simunic, D., & Prasad, R. (2012). Effects of malicious attacks in mobile ad-hoc networks. In *Proceeding of the 2012 IEEE international conference on computational intelligence and computing research*, December 2012, Coimbatore, India.
16. Himral, L., Vig, V., & Chand, N. (2011). Preventing AODV routing protocol from black hole attack. *International Journal of Engineering Science and Technology, 3*(5), 3927–3932.
17. Sivasankar, P., Chellappan, C., & Balaji, S. (2011). Performance of energy efficient routing protocol for MANET. *International Journal of Computer Applications, 28,* 1–6.
18. Mahmaud, M., et al. (2013). Secure and reliable routing protocols for heterogeneous multihop wireless networks. *IEEE Transactions on Parallel and Distributed Systems, 1,* 11.
19. Goldsmith, A., & Wicker, S. (2002). Design challenges for energy constrained ad-hoc wireless networks. *Wireless Communications, 9*(4), 8–27.
20. Ray, N. K., & Turuk, A. (2010) Energy efficient technique for wireless Ad hoc network. In *Proceeding of the international joint conference on information and communication technology* (pp. 105–111).
21. Johnson, D. B., & PalChaudhuri, S. (2008). Power mode scheduling for Ad Hoc networks. *Proceedings of the International Conference on Network Protocols, 19*(5), 192–193.
22. Souihli, O., Frikha, M., & Mahmoud, B. H. (2009). Load-balancing in MANET shortest-path routing protocols. *Ad Hoc Networks, 7*(2), 431–442.
23. Shu, T., Krunz, M., & Liu, S. (2010). Secure data collection in wireless sensor networks using randomized dispersive routes. *IEEE Transactions on Mobile Computing, 9*(7), 941–954.
24. Sun, H., Chen, C., & Hsiao, Y. (2007). An efficient countermeasure to the selective forwarding attack in wireless sensor networks. *Proceeding of the IEEE TENCON, 2007,* 1–4.
25. Y. Zhang, S. He, & J. Chen (2015). Data gathering optimization by dynamic sensing and routing in rechargeable sensor networks. *IEEE/ACM Transactions on Network*. https://doi.org/10.1109/tnet.2015.2425146.
26. Lou, W., & Kwon, Y. (2006). H-spread: A hybrid multipath scheme for secure and reliable data collection in wireless sensor networks. *IEEE Transactiononvehicular Technology, 55*(4), 1320–1330.
27. Liu, Y., Zhu, Y., Ni, L. M., et al. (2011). A reliability-oriented transmission service in wireless sensor networks. *IEEE Transactions on Parallel and Distributed Systems, 22*(12), 2100–2107.
28. Hu, Y., & Liu, A. (2015). An efficient heuristic subtraction deployment strategy to guarantee quality of event detection for WSNs. *The Computer Journal, 58*(8), 1747–1762.
29. Yu, Y. L., Li, K. Q., Zhou, W. L., & Li, P. (2012). Trust mechanisms in wireless sensor networks: Attack analysis and counter measures. *Journal of Network and Computer Applications, 35*(3), 867–880.
30. Punithavathani, D. S., Sujatha, K., & Jain, J. M. (2015). Surveillance of anomaly and misuse in critical networks to counter insider threats using computational intelligence. *Cluster Computing, 18*(1), 435–451.

31. Douss, A. B. C., Abassi, R., & El Fatmi, S. G. (2014) A trust management based security mechanism against collusion attacks in a MANET environment. In *2014 ninth international conference on availability, reliability and security (ARES)* (pp. 325–332). New York: IEEE.
32. Xia, H., Jia, Z., Li, X., Ju, L., & Sha, E. H.-M. (2013). Trust prediction and trust-based source routing in mobile ad hoc networks. *Ad Hoc Networks, 11*(7), 2096–2114.
33. Rump, F., Jopen, S. A., & Frank, A. (2016) Using probabilistic multipath routing to improve route stability in MANETs. In *2016 IEEE 41st conference on local computer networks (LCN)* (pp. 192–195). New York: IEEE.
34. Meghanathan, Natarajan. (2011). A location prediction based routing protocol and its extensions for multicast and multi-path routing in mobile ad hoc networks. *Ad Hoc Networks, 9*(7), 1104–1126.
35. Souihli, O., Frikha, M., & Mahmoud, B. H. (2009). Load-balancing in MANET shortest-path routing protocols. *Ad Hoc Networks, 7*(2), 431–442.
36. DasGupta, S., Saha, S., Bhowal, D., & Bhowmik, D. (2010) LBSPR: Location based shortest path routing protocol in MANET. In *2010 IEEE international conference on computational intelligence and computing research (ICCIC)* (pp. 1–4). New York: IEEE.
37. Deng, Xiaoheng, Peng, Qionglin, He, Lifang, & He, Tingting. (2016). Interference-aware QoS routing for neighbourhood area network in smart grid. *IET Communications, 11*(5), 756–764.
38. Deng, Xiaoheng, Lifang He, Xu, Li, Qiang Liu, Cai, Lin, & Chen, Zhigang. (2016). A reliable QoS-aware routing scheme for neighbor area network in smart grid. *Peer-to-Peer Networking and Applications, 9*(4), 616–627.
39. Zhan, G. X., Shi, W. S., & Deng, J. L. (2012). Design and implementation of TARF: A trust-aware routing framework for WSNs. *IEEE Transactions on Dependable and Secure Computing, 9*(2), 184–197.
40. Hsieh, M. Y., Huang, Y. M., & Chao, H. C. (2007). Adaptive security design with malicious node detection in cluster-based sensor networks. *Computer Communications, 30*(1), 2385–2400.
41. He, D., Chen, C., Chan, S., Bu, J., & Vasilakos, A. V. (2012). ReTrust: Attack-resistant and lightweight trust management for medical sensor networks. *IEEE Transactions on Information Technology in Biomedicine, 16*(4), 623–632.
42. Gómez Mármol, F., & Martínez Pérez, G. (2012). TRIP, a trust and reputation infrastructure-based proposal for vehicular ad hoc networks. *Journal of Network and Computer Applications, 35*(3), 934–941.
43. Deno, M., & Sun, T. (2008). Probabilistic trust management in pervasive computing. In *Proceedings of the international conference on embedded and ubiquitous computing*, 17–20 December 2008 (Vol. 2, pp. 610–615).
44. Zia, T. (2008). Reputation-based trust management in wireless sensor networks. In *Proceedings of the international conference on intelligent sensors, sensor networks and information processing*, December (Vol. 15–18, pp. 163–166).
45. Mahmaud, M., et al. (2013). Secure and reliable routing protocols for heterogeneous multihop wireless networks. *IEEE Transactions on Parallel and Distributed Systems, 1,* 11.
46. Pirzada, A., Datta, A., & McDonald, C. (2004). Trust-based routing for ad-hoc wireless networks. *Proceedings of the International Conference on Networks, 1,* 326–330.
47. Li, X., Lyu, M., & Liu, J. (2004) A trust model based routing protocol for secure ad-hoc networks. In *Proceeding of the aerospace conference*, 6–13 March 2004 (Vol. 2, pp. 1286–1295).
48. Marchang, N., & Datta, R. (2012). Light-weight trust-based routing protocol for mobile ad-hoc networks. *Information Security, 6*(2), 77–83.
49. Aad, I., Hubaux, P. J., & Knightly, W. E. (2008). Impact of denial-of-service attacks on ad-hoc networks. *IEEE-ACM Transactions on Networking, 16*(4), 791–802.
50. Gómez Mármol, F., & Martínez Pérez, G. (2012). TRIP, a trust and reputation infrastructure-based proposal for vehicular ad hoc networks. *Journal of Network and Computer Applications, 35*(3), 934–941.

51. Wang, J., Liu, Y. H., & Jiao, Y. (2011). Building a trusted route in a mobile ad hoc network considering communication reliability and path length. *Journal of Network and Computer Applications, 34*(4), 1138–1149.
52. Jaspal, K., Kulkarni, M., & Gupta, D. (2013). Effect of black hole attack on MANET routing protocols. *IJ Computer Network and Information Security, 5,* 64–72.
53. Hong, X., Kong, J., & Gerla, M. (2006). *Mobility changes anonymity: New passive threats in mobile ad hoc networks, Special issue on wireless network security*. New York: Wiley Interscience Press.
54. Divecha, B., Abraham, A., Grosan, G., & Sanyal, S. (2007). Impact of node mobility on MANET routing protocols models. *Journal of Digital Information Management, 4*(1), 19–23.
55. Divecha, B., Abraham, A., Grosan, G., & Sanyal, S. (2007). Impact of node mobility on MANET routing protocols models. *Journal of Digital Information Management, 4*(1), 19–23.
56. Sharma, M., Khare, S., Dixit, N., & Agrawal, S. (2012). Security in routing protocol to avoid threat of black hole attack in MANET. *VSRD-IJEECE, 2*(6), 385–390.
57. Divecha, B., Abraham, A., Grosan, G., & Sanyal, S. (2007). Impact of node mobility on MANET routing protocols models. *Journal of Digital Information Management, 4*(1), 19–23.
58. Jerome, H., Filali, F., & Bonnet, C. (2009). Mobility models for vehicular ad hoc networks: A survey and taxonomy. *Communications Surveys and Tutorials, IEEE, 14,* 19–41.
59. Guolong, L., Noubir, G., & Rajaraman, R. (2004) Mobility models for ad hoc network simulation. In *Twenty-third annual joint conference of the IEEE computer and communications societies*, INFOCOM 2004, (Vol. 1). New York: IEEE.

R. Tino Merlin was born in Nagercoil, India. She received the B.E. degree in Computer science and Engineering from St. Xavier's Catholic College of Engineering affiliated to Anna University, Chennai, India, in 2007, and the M.E degree in Computer Science and Engineering from Francis Xavier Engineering College affiliated to Anna University Chennai, India, in 2009 and currently pursuing her Ph.D. degree in Computer Science and Engineering from the Anna University, Chennai, India respectively. She is having more than 4 years of academic experience in Engineering Institution. She is also life member of Indian Society for Technical Education. Her current research interests includes Networks, Network Security, Mobile Ad hoc Networks, Cyber Security and Wireless Routing. She has published various international journals and attended many national conferences.

Dr. R. Ravi is an Editor in International Journal of Security and its Applications (South Korea). He is presently working as a Professor and Head of the Department of IT, and Research Centre Head of the CSE Department in Francis Xavier Engineering College, Tirunelveli. He completed his B.E in Computer Science and Engineering from Thiagarajar College of engineering, Madurai in 1994 and M.E in CSE from Jadavpur Government research University, Kolkata. He has completed his Ph.D. in Networks from Anna University Chennai. He has 23 years of experience. He is the first person in India from a private institution who was the judge (Chair person) for an International conference in IIT, Chennai. He published 58 International/National Journals, and 4 international Journals are under process. He actively participated in 31 international Conference, 98 National Conferences and bagged shields in many. He is also a fulltime recognized guide for vari-

ous Universities. Currently he is guiding nine research scholars. His areas of interest are Virtual Private networks, Image Processing, Neural Network.