Defense against Sybil attacks and authentication for anonymous location-based routing in MANET

S. Vadhana Kumari[1] · B. Paramasivan[2]

Published online: 9 January 2016

Abstract In MANET, providing authentication and security to location-based routing is a big task. To overcome this problem, in this paper, we proposed a defense against Sybil attacks and authentication for anonymous location-based routing in MANET. Each random forwarder has a table of RSS values estimated from the previous message exchanges across a zone to detect the Sybil attack. The difference in RSS values of two neighboring nodes is estimated based on which the node's arrival angle into the zone is detected. Depending on the arrival angle, the nodes can be categorized as safety zone and caution zone. The messages exchanged between the RFs and senders can be protected by means of group signature. Finally, misrouting packet drop attack is detected and eliminated by using ant colony optimization technique. By simulation results, we show the proposed technique reduces the packet drop due to attacks, thereby increasing the delivery ratio.

Keywords Mobile ad hoc network · Routing · Ant colony optimization · Network topologies · Authentication · Attacks

1 Introduction

Mobile ad hoc network (MANET), a self-organizing independent communication infrastructure, is a collection of mobile nodes equipped with a wireless transmitter and a receiver. Nodes can dynamically and freely self-organize into arbitrary and temporary ad hoc network topologies to communicate with each other within its transmission range via bidirectional wireless links either directly or indirectly without any central infrastructure. The node relays on other nodes to communicate with nodes outside its transmission range. MANET has its applications in commerce, emergency services, military, education, e-health, the tactical networks, rescue operation, communication, and entertainment [1–5, 7, 8, 10, 22–26].

As the nodes lack physical protection, malicious attackers can easily capture and compromise nodes to achieve attacks, that is, generally routing protocols considers how every node in the network behaves with other nodes and not maliciousness; hence, attackers can easily compromise MANETs by inserting malicious or non-co-operative nodes into the network [1, 27–31].

The dynamic nature of MANET makes it highly susceptible to several link attacks. Security based routing protocols must ensure confidentiality, availability, authenticity, and integrity. Most of the existing security solutions for wired networks are inefficient in MANET environment since the transmission occurs in open medium causes security attacks. The effect of various attacks can be reduced due to the presence of security protocol. In MANET, the nodes with insufficient physical protection may become malicious and reduce the network performance. Even though all routing protocols assume that nodes provide secure communication, some nodes become malicious that disrupt the network operation by altering routing information [32–37].

✉ S. Vadhana Kumari
vadhanakumari0371@gmail.com

[1] Department of Computer Science and Engineering, Maria College of Engineering and Technology, Attoor, Tamilnadu, India

[2] Department of Computer Science and Engineering, National Engineering College, Kovilpatti, Tamilnadu, India

MANETs are subjected to two levels of attacks. The first level of attack happens during basic mechanisms such as routing, whereas the second one damages the security mechanisms used in the network. Attacks are divided into two major types: internal and external. Internal attacks are directly led to the attacks on nodes presents in network and links interface between them, whereas external attacks prevent the network from normal communication and producing additional overhead to the network [38–41]. External attacks are further divided as passive and active attack. Passive attacks do not alter the data transmitted within the network, whereas active attacks are severe on the network as it prevents message flow between the nodes [42, 43].

Sybil attacks pose a serious threat though MANETs need a unique, distinct, and persistent identity per node for their security protocols to networks. It occurs in network layer. A Sybil attacker can either create more than one identity on a single physical device to launch a coordinated attack on the network or can switch identities to weaken the detection process, thereby promoting lack of accountability in the network [3]. There are also attacks like neighbor attack, jelly fish attack, replay attack and denial of service attack [11–14, 44].

In MANET, employing a high-cost anonymous routing in a battlefield, a low quality of service in voice and video data transmission due to depleted resources may lead to disastrous delay in military operations [2, 45–47].

There is no combined mechanism for preventing Sybil attacks and providing authentication in case of location-based routing. Moreover, most of the existing attack detection techniques did not consider the quality of service parameters. In ALERT, although source and destination anonymity protection is provided, it suffers from Sybil attack. A Sybil attacker can disrupt location-based or multipath routing by participating in the routing, giving the false impression of being distinct nodes on different locations or node-disjoint paths [2]. The attackers can be battery powered nodes that passively receive network packets and detect activities in their vicinity. They can also be powerful nodes that pretend to be legitimate nodes and inject packets to the network according to the analytical results from their eavesdropped packets. Moreover, the routing and control messages exchanged by the nodes can be fabricated or altered. Hence, efficient authentication is required to ensure the integrity.

To overcome this issue, in this paper, defense against Sybil attacks and authentication for anonymous location-based routing is proposed in MANET.

The paper is organized as follows. Section 2 describes the related works and Sect. 3 provides the detailed explanation of the proposed work. Section 4 explains the simulation results. Finally, Sect. 5 concludes the work.

2 Literature review

Shengrong Bu et al. [6] have presented a distributed scheme combining authentication and intrusion detection where the most suitable biosensors for authentication or IDSs are dynamically selected based on the current security posture and energy states. Dempster–Shafer theory has been used for IDS and sensor fusion to enhance the concept as multiple devices are used at a time slot. The problem has been formulated as a POMDP multi-armed bandit problem, and its optimal policy can be chosen using Gittins indexes. The distributed multimodal biometrics and IDS scheduling process can be divided into offline and online parts to mitigate the computational complexity. Simulation results show that this scheme improves network security. Such methods of combining multiple sensor information in a distributed fashion lend themselves well to the concept of cross-layer security, which is a topic that is gaining interest in MANET security. However, there is computational complexity.

Boppana and Su [8] have presented quantitative evaluations of false positives and their impact on monitoring based intrusion detection for ad hoc networks. Experimental results showed that even for a simple three-node configuration, an actual ad hoc network suffers from high false positives; these results are validated by Markov and probabilistic models. However, this false positive problem cannot be observed by simulating the same network using popular ad hoc network simulators, such as NS-2, OPNET, or Glomosim. A probabilistic noise generator model implemented in the Glomosim simulator for recovery, and the simulated network exhibits the aggregate false positive behavior similar to that of the experimental test bed with this model. Simulations of larger (50-node) ad hoc networks indicate that monitoring-based intrusion detection has very high false positives. These false positives can reduce the network performance or increase the overhead. In a simple monitoring-based system where no secondary and more accurate methods are used, the false positives impact the network performance in two ways: reduced throughput in normal networks without attackers and inability to mitigate the effect of attacks in networks with attackers. However, there are passive monitoring issues.

Li and Liu [9] have presented a fully distributed ID-based multiple secrets key management scheme (IMKM) implemented through a combination of ID-based multiple secrets and threshold cryptography. The certificate-based authenticated public key distribution requirement is eliminated by this, and an efficient mechanism is provided for key update and key revocation schemes leading to more suitable, economic, adaptable, scalable, and autonomous key management for MANET. However, the average completion time for the key update process is very large in terms of different cluster sizes and speeds.

Ayday and Fekri [10] have developed an iterative malicious node detection mechanism for delay/disruption tolerant networks (DTNs) referred as ITRM, which is a graph-based iterative algorithm motivated by the prior success of message passing techniques for decoding low-density parity-check codes over bipartite graphs. The iterative reputation management scheme far more effective than well-known reputation management techniques like Bayesian framework and Eigen Trust by applying ITRM to DTNs for various mobility models provides high data availability and packet-delivery ratio with low latency in DTNs under various adversary attacks attempting to both undermine the trust and detection scheme and the packet delivery protocol.

Khalil and Bagch [15] have presented stealthy attacks in wireless ad hoc networks: detection and counter measure (SADEC), a protocol presenting two techniques based on local monitoring, that is, neighbors maintaining extra information of routing path, and adding some checking responsibility to each neighbor, to detect and isolate stealthy packet dropping attack efficiently. SADEC provides an innovative mechanism to better utilize local monitoring by considerably increasing the number of nodes in a neighborhood that can do monitoring. Baseline local monitoring fails to efficiently mitigate most of the presented attacks while SADEC successfully mitigates them. However, the listening activity for detecting malicious behavior is more complicated due to the presence of multiple channels and multiple radios.

van der Merwe et al. [16] have proposed a public key management service called trustworthy key management for MANET (AdHocTKM) taking the advantages of threshold cryptography and certificate chaining and integrates it with self-certified public keys and self-certificates to yield a key management service that is secure, trustworthy and highly available to users. Cryptographic key issuing protocol allows negotiation between a single entity and a distributed authority for an implicit self-certified public key, without the authority gaining knowledge of the corresponding private key. This algorithm is called as threshold self-certified public keying.

From the literature review done, we can observe that there is no fixed security architecture which provides defense against various attacks as well as provide authentication for routing and data packets in MANET.

3 Proposed solution

3.1 Overview

In this paper, to detect the Sybil attack, each random forwarder has a table of RSS values estimated from the previous message exchanges across a zone. The difference in RSS values of two neighboring nodes are estimated based on which the node's arrival angle into the zone is detected. Then depending on the arrival angle, the nodes can be categorized into safety zone and caution zone. Based on the mean value of RSS of all the nodes in safe zone, a safety threshold (ST) is estimated and further transmission is compared against this safety threshold. The nodes whose RSS difference is larger than the safety threshold are considered as abnormal nodes and are put under the caution zone. This scheme works better even in mobile environments and can detect both join-and-leave and Sybil attackers with a high degree of accuracy.

The messages exchanged between the Forwarders and senders can be protected by means of group signature. In group signature scheme, any member of a large and dynamic group can sign a message, thereby producing a group signature. A group signature can be verified by anyone who has a copy of a constant-size group public key. A valid group signature implies that the signer is a genuine group member. In ALERT, each mobile node periodically signs its current location (link-state) information which will be verified by the RFs and destination. Ant colony optimization (ACO) technique is used to establish a route from source and destination. When the packet is sent to the wrong next hop, misrouting packet drop attack may happen. This attack can be detected and eliminated by incorporating the identity information of nodes in the ant agent.

3.2 RSS based on arrival angle

The protection against Sybil attack is provided by received signal strength (RSS) [4] values. RSS is used to estimate the distance between the destination node and neighboring node [18]. Each node will capture and store the signal strength of the transmissions received from its neighboring nodes in the RSS value table. In MANET, the nodes move dynamically. The position of nodes changes according to the time interval. Each node has different RSS values in different timings. The RSS difference (DRSS) value is calculated as

$$DRSS = \frac{T_2 - T_1}{t_2 - t_1} \tag{1}$$

In Eq. (1), T_2 is the RSS value at time t_2 and T_1 is the RSS value at time t_1. The RSS table is shown in the Table 1.

In Table 1, status field is binary either 0 or 1. If the node is malicious node, then value will be 1. If the node is not

Table 1 RSS value table

Node ID	Neighboring node	RSS value		Status
		t_2	t_1	

malicious, then value will be 0. The table contains the RSS values at time t_1 and t_2. Malicious node is detected using Algorithm 2. Consider the network shown in Fig. 1:

In Fig. 1, a sample network is shown. In that network, each node has many neighboring nodes, and they change their position dynamically. Consider node B has node X, P, M, U, Z, and C as neighboring nodes.

In Fig. 2, four neighboring nodes are entering into the coverage area of node B.

The zone within the node's coverage area is termed as stable zone, and the zone at the boundary of the coverage area is termed as caution zone. The node's arrival angle θ is the angle at which a neighboring node enters the coverage area of a target node, which is calculated using DRSS. The critical angle θ_a is defined as the arrival angle so that when a neighboring node arrives at this angle, it remains in the caution zone without getting into the stable zone. Critical angle is useful to decide the angle of a neighboring node. In Fig. 2, when the neighboring nodes (C, Z, M and U) enter into the coverage area of node B, then it remains in the caution zone. Zone selection and metric value calculation is explained in the algorithm given below.

```
1.  Start
2.  Calculate the DRSS value using equation (1)
3.  Calculate the neighboring node arrival angle θ
4.  Compare the arrival angle with the critical angle
5.  When the neighbor node enters the "caution zone", it compares the arrival angle with critical angle
6.      If (θ < θa)
        {
              then metric value = 1 (node Z in figure 2)
        }
7.      else (i.e. θ ≥ θa)
        {
    then metric value = -1 (node U in figure 2)
}
8.      If (neighbor node stays in the safety zone)
        {
    then metric value is set as 2 (node C in figure 2)
         }
9.      Else (neighbor node leaves the safety zone)
        {
    then metric value = -2 and consider the node as bad neighbor (node M in figure 2)
        }
10. Select the forwarding nodes having metric value greater than zero
11. End
```

Algorithm 1: Zone Selection and Metric Value Calculation

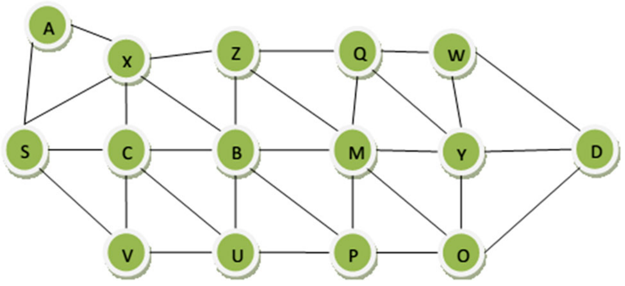

Fig. 1 Sample network

The metric value is used to determine the quality of the neighboring nodes considering the estimated arrival angle. This metric is included in the RREQ packet. This metric is called as minimum link metric along the path. The metric is decided using Table 2.

When the neighboring node is entering into the caution zone angle θ, it is compared with the arrival angel. If the $\theta < \theta_a$, then the metric value will be 1. If $\theta \geq \theta_a$, then the metric value will be −1. If the neighboring node is located in the safety zone, then the metric value will be 2. If the neighboring node leaves the safety zone, then the metric value will be −2. It will consider as bad neighbor node.

RSS threshold value is calculated as

$$TV = \sum_{i=1}^{n} \mathrm{RSS}_t \tag{3}$$

In Eq. (3), TV is the RSS threshold value. If the node RSS value is greater than the RSS threshold value, then it is considered as malicious node and the value 1 is added to the status field in Table 1. A broadcast message is send to the all remaining nodes about the malicious node. Each node has RSS value and all nodes RSS values are added to the table using the algorithm given below.

```
Start
Define add = Address of the node
        T = time received
Each node has address, RSS value and time T
If (node address present in the table)
{
    If (node. RSS $\geq$ TV)
    {
            Add 1 to status field in  table 1
            Broadcast node as Malicious node and update the table
    }
    Else
            Add the node to neighbor table
}
Else
    {
            Create a new record (node add, RSS, T) and a link list is created to store the address
    }
When the link list reaches the maximum value, the older RSS values are removed from the list
End
```

Algorithm 2: Adding node to the RSS table

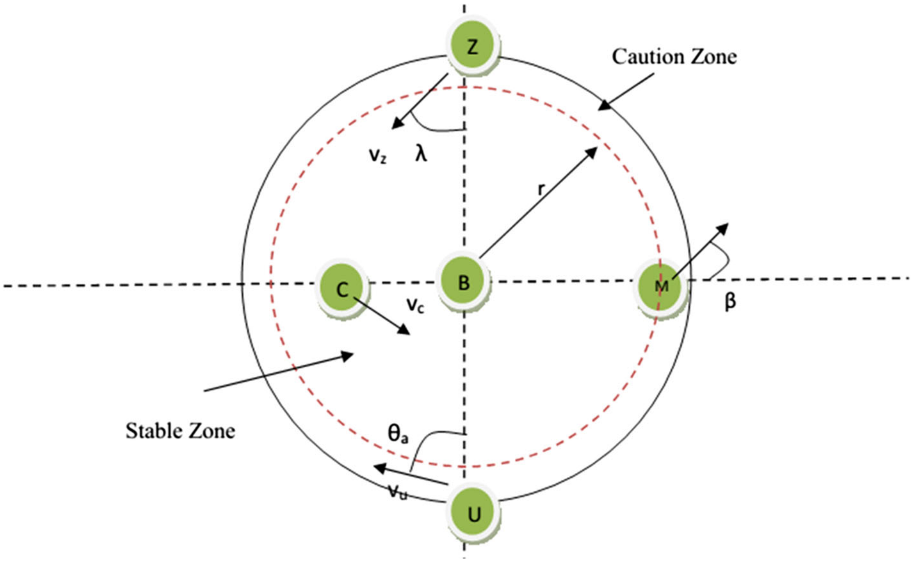

Fig. 2 Calculating node's arrival angle

In algorithm (2), if the node address does not exist in the table (this node has not been interacted with before), then a new record is created and the node address is added. Each node has the address, RSS value and timer. Each node calculates the RSS value for end of timer. The new value is updated in the table. Sybil attack detection is explained in the algorithm given below.

```
Start
Define TI = RSS Timer
        Temp = contain the nodes whose RSS value are not updated
        TV = threshold value
If ( TI is completed)   // RSS time out
{
      For each address in the table, update the RSS values
      If ( we did not get any node RSS value)
              Temp = add all node address to this value
}
Get the previous RSS values of nodes in temp
If (node RSS > TV)
      Add the node as a malicious node
Else
      Node is out of range
End
```

Algorithm 3: Sybil Attack Detection

Table 2 Metric value

Arrival angle (θa)	Neighboring node angle (θ)	Caution zone		Safety zone
		$\theta < \theta$a	$\theta \geq \theta$a	
		1	−1	2

In algorithm (3), the RSS values of each node are updated for time in timer. If any node RSS value is not updated then those is added to temp list. Get the previous RSS values for the nodes in the temp list and compare with the threshold value. If the nodes have RSS value more than the threshold value, those nodes are added as the malicious node. Otherwise, that node is out of range.

3.3 Group signature with self-distinction

Group signatures are defined as public key signatures with additional privacy features. The messages exchanged between the random forwarders (RFs) and senders can be protected by means of group signature. Group signature can easily be verified by the one who has a copy of a constant-size group public key. The signature is valid, only when the signer is a genuine group member. Group signature scheme [17] is used to protect the network against attacks by outsiders and passive (honest-but-curious) insiders. Self-Distinction is a special feature that is used to underlying the group signature, when the resistance to Sybil attack is needed. Self-Distinction provide the node privacy across time slots is still preserved, but it is disagree with what group signatures try to achieve anonymity and unlinkability.

This approach is different with all group signature methods. In this method, each node in the group has a common random number that is generated by random number generator. That random number is changed for each round of signing. If any node uses same random number sign twice, then it consider as the affected node. Two examples of group signatures with self-distinction are [18] and [19]. It is unscalable to maintain a group key as a common parameter. Another efficient approach is Sequential Aggregate Signatures (SAS).

3.3.1 *Sequential aggregate signatures (SAS)*

Each node uses its private key to sign other forwards packets. These signatures can be aggregated to maintain a constant aggregate signature in the node. If an attacker attacks the network by impersonating the other nodes, then it will detected due to mismatching signatures in received forwarded packets.

All these sequential aggregate signatures [17] are constant in size and this SAS is constructed based on RSA [20] and its signature generation is equivalent to a plain RSA signature. The cost of verification is increases linearly with number of signers on the path and this cost is minimized using the small public exponents. SAS is explained as follows.

1. *Step 1* Each node has one private key and one public key. Node private key is $\mathrm{PRK_i} = \mathrm{P_i}$ and pair of public key is $\mathrm{PUK_i} = (\mathrm{n_i}, \mathrm{m_i})$.
2. *Step 2* In SAS is expanded by t bits $\mathrm{S_1}, \mathrm{S_2}, \mathrm{S_3}, \ldots, \mathrm{S_t}$ and t is the number of signers in the aggregate signature.
3. *Step 3* In this process, if the ith signature is $\mathrm{Z_i} \geq \mathrm{n_{i+1}}$, then $\mathrm{S_i}$ is set to 1. Otherwise, it is set 0. In the verification phase, if $\mathrm{S_i}$ is 1 then n_{i+1} is added to the Z_i before proceeding with the verification of Z_i. Z_i is the normal public key signature.

These three steps are required to generate a sequential aggregate signature. It is explained with the example given in Fig. 3.

Assume S wants to send the packets to destination D. In between the sender and destination, two neighboring nodes B and C are present. S sends the packets to the D through the B and C.

Fig. 3 Example for sequential aggregate signatures

At node S: S computes the $h_s = H(n_s, m_s)$ and $\mathrm{Z}_s = (h_s)^{p_s}(\mathrm{mod}s)$. Z_s is added to the packet.

At node B: If $\mathrm{Z}_s \geq n_b$, set $\mathrm{Z}_s = \mathrm{Z}_s - n_B$ $\mathrm{S}_1 = 1$ else $\mathrm{S}_1 = 0$ compute $h_B = H(n_B, m_B)$ and $\mathrm{Z}_{SB} = (h_s + h_B)^{S_B}$ $(\mathrm{mod}n_s)$. Z_{SB} is added instead of Z_s.

At node C: If $\mathrm{Z}_{SB} \geq n_C$, set $\mathrm{Z}_{SB} = \mathrm{Z}_{SB} - n_C$ $\mathrm{S}_2 = 1$ else $\mathrm{S}_2 = 0$ compute $h_C = H(n_c, m_c)$ and $\mathrm{Z}_{SBC} = (h_B + h_C)^{S_C}$ $(\mathrm{mod}n_C)$. Z_{SBC} is added instead of Z_{SB}.

At node D:

$$h_C = H(n_c, m_c),$$

$$\mathrm{Z}'_{SB} = \mathrm{Z}^{m_c}_{SBC} - h_C(\mathrm{mod}n_C)$$

$$\mathrm{Z}_{SB} = \mathrm{Z}'_{SB} + b_2 n_c,$$

$$path_B = H(n_B, m_B),$$

$$\mathrm{Z}'_S = \mathrm{Z}^{m_B}_{SB} - h_B(\mathrm{mod}n_B),$$

$$\mathrm{Z}_S = \mathrm{Z}'_S + b_1 n_B,$$

$$h_S = H(n_S, m_S)$$

And finally $\mathrm{Z}^{Y_S}_S(\mathrm{mod}n_S)$ is equal to h_S. If the signature did not match then the packets choose another path.

3.4 Packet drop attack detection

Stealthy packet dropping [21] disrupts the packet from reaching the destination through malicious behavior at an intermediate node. This can occur due to misrouting of packets in which the intermediate node relays the packet to the wrong next hop. This can be avoided by including the identity of the next hop for the packet being relayed at each guard. The routing table is created with the identity information, source address, and destination address. The routing table is shown in Table 3. The identity is collected during route discovery. Each packet header contains the identity information, so that it does not create any additional traffic in the network. Guard nodes are the group of

Table 3 Simulation parameters

No. of nodes	50, 100, 150 and 200
Area size	500 × 500
Mac	IEEE 802.11
Transmission range	250 m
Simulation time	20 s
Traffic source	CBR
Packet size	512
Sources	4
Attackers	4
Rate	50 kb
Speed	2, 4, 6, 8 and 10 m/s

nodes that performs local monitoring for detecting security attacks.

When a source node wants to send a message to some destination node and does not already have a valid route to that destination, it initiates a route discovery process to locate the other node. The route discovery is done by using ant colony optimization (ACO) technique.

3.4.1 Ant based route discovery for detection

Ant colony optimization (ACO) technique is used here to discover the route from the source to the destination. Forward ant agent (FA) establishes the pheromone path to the source while backward ant agent (BA) establishes the pheromone path to the destination. These ant agents collect the identity information of each node that is required for mitigating misrouting packet drop. When FA reaches the destination, BA is created and information gathered in FA is transferred to BA. BA traverses in the same path but in the opposite direction of FA and updates the path information at all the intermediate nodes.

Source node creates FA with source address and broadcasts it to the neighbor nodes in the network. After receiving the FA, the neighbor node verifies the destination address of FA. If the destination address of FA is not similar, then it adds its own address, destination address and identity from the routing table and broadcasts it to its neighbor nodes. In order to gather the next-hop identity information, the forwarder of the FA attaches the previous two hops to the packet header. From Fig. 3, the previous hop of C is B for a route from source S to destination D, and the next hop from C is H. Node C broadcasts the FA with the identity of B and its own identity in the packet header.

The format of the FA packet header is given by: <S: D: id (B): id (C)>.

When H and the other neighbors of C get the FA from C, they keep in a verification table (VT). The format of FA information stored in VT are <S: D: id (B): id(c): _>. In this table, the last field is left blank. When H broadcasts the FA, the common neighbors of C and H update their VT to include H. Then the format of VT becomes <S: D: id(B): id(C): id(H)>.

When H receives a BA to be relayed to C, H includes the identity of the node in BA that C needs to communicate to B. Therefore, all the guards of C know that C not only needs to forward the BA but also that it should forward it to B.

Guards have the responsibility to monitor the BA agent. First, the guard G of a node C verifies that C forwards the BA to the correct next hop. Second, G verifies that node C has updated the forwarded BA header correctly. The format of BA packet header, when the input packet to B from C is <BA: S: D: id(H): id(C): id(B)>, then the output BA packet format from B should be <BA: S: D: id(C): id(B): id(S)>.

Using the information collected by ant agents, the misrouting attacks can be detected as follows. Assume that source S wants to send a data packet to destination D through a route that includes <S B C H D>. Let us consider that C be the malicious node. Here, C cannot misroute the data packet received from B to a node other than the next hop, as each guard of C over the link C–H has an entry in its VT. VT indicates H as the correct next hop. This is due to the additional checking of the guard node. In addition, C cannot frame another neighbor E, by misrouting the packet to E as the guards of E over link C–E do not have an entry like <S: D: id(B): id(C): id(E)> (Fig. 4).

Algorithm 4

```
1. Source S creates FA with source and destination address
2. After getting the packet, the neighbor node stores the packet header of FA in Verification Table (VT)
3. The forwarder of FA attaches identity of previous two hops and then sent it to the next hop
4. For each hop, guard checks whether it has identity in packet header
   {
5.         If (identity of the node present)
           {
6.                 If (node ≠ destination)
                       {
7.                             Repeat the Step 3 and 4
                       }
8                  Else
                       {
9.                             Destination sends the backward ant (BA) to source
10.                            Guard update the BA packet header at each hop
                       }
11.        Else
                   Node discards the FA packet
       }
```

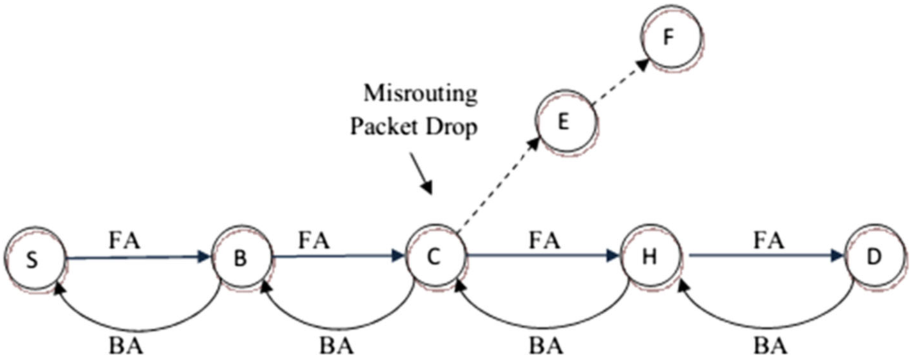

Fig. 4 Route discovery using ACO

4 Simulation results

4.1 Simulation model and parameters

The network simulator (NS-2) [21] version 2.32 is used to simulate the proposed architecture. In the simulation, the mobile nodes move in a 500 meter × 500 meter region for 20 s of simulation time. All nodes have the same transmission range of 250 meters. The simulated traffic is Constant Bit Rate (CBR).

The simulation settings and parameters are summarized in Table 3.

4.2 Performance metrics

The proposed defense against Sybil attacks and authentication for anonymous location-based routing (AALBR) is compared with the ALERT [2] and ALARM [17] techniques. The performance is evaluated for packet delivery ratio, packet drop and overhead metrics.

4.3 Results

(a) Varying the number of nodes

The number of mobile nodes is varied as 50,100,150 and 200 with a speed of 2 m/s and performance is evaluated.

Figures 5, 6 and 7 show the results of packet delivery ratio, packet drop and overhead for the 3 techniques, when the number of nodes is increased. From the figures, it can be observed that AALBR outperforms the other two techniques in terms of all the metrics. It attains 8 and 21 % higher delivery ratio when compared to ALERT and ALARM. Similarly it has reduced packet drops by 66 and 81 % compared to ALERT and ALARM. The overhead of AALBR is 90 and 80 % less when compared to ALERT and ALARM.

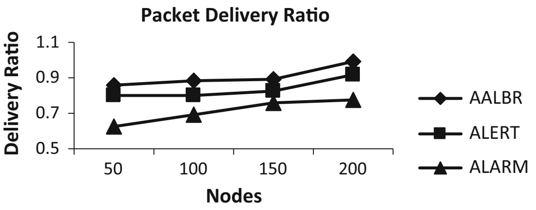

Fig. 5 Nodes versus delivery ratio

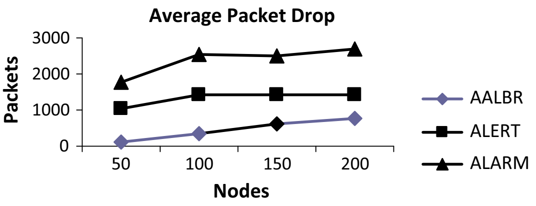

Fig. 6 Nodes versus drop

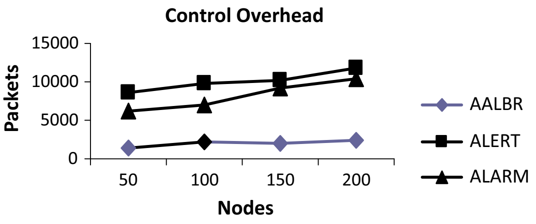

Fig. 7 Nodes versus overhead

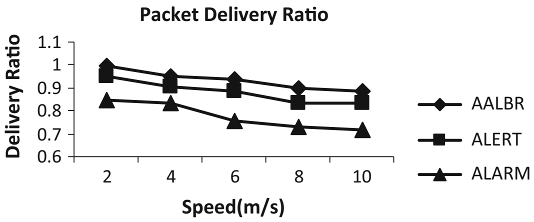

Fig. 8 Speed versus delivery ratio

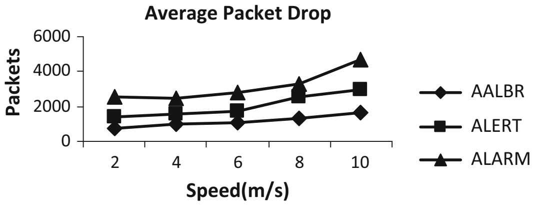

Fig. 9 Speed versus drop

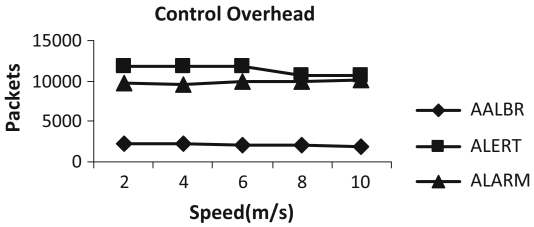

Fig. 10 Speed versus overhead

(b) Varying the node speed

The speed of 100 mobile nodes is varied as 2, 4, 6, 8 and 10 m/s and the performance is evaluated.

Figures 8, 9 and 10 show the results of packet delivery ratio, packet drop and overhead for the 3 techniques, when the node speed is increased. From the figures, it can be observed that AALBR outperforms the other two techniques in terms of all the metrics. It attains 6 and 17 % higher delivery ratio when compared to ALERT and ALARM. Similarly it has reduced packet drops by 42 and 62 % compared to ALERT and ALARM. The overhead of AALBR is 81 and 78 % less when compared to ALERT and ALARM.

5 Conclusion

In this paper, we have proposed a defense against Sybil attacks and authentication for anonymous location-based routing in MANET. To detect the Sybil attack, each node has a table of RSS values estimated from the previous message exchanges across a zone. Then depending on the arrival angle, the nodes can be categorized into safety zone and caution zone. Based on the mean value of RSS of all the nodes in safe zone, a safety threshold is estimated and further transmission is compared against this safety threshold. The messages exchanged between the RFs and senders can be protected by means of group signature. In group signature scheme, any member of a large and dynamic group can sign a message, thereby producing a group signature. A valid group signature implies that the signer is a genuine group member. Finally, misrouting packet drop attack is detected and eliminated by using ant colony optimization (ACO) technique. This scheme works better even in mobile environments and can detect both join-and-leave and Sybil attackers with a high degree of accuracy along with the detection of misrouting packet drop arrack.

References

1. Shakshuki, E. M., Kang, N., & Sheltami, T. R. (2013). EAACK—A secure intrusion-detection system for MANETs. *IEEE Transactions on Industrial Electronics*, *60*(3), 1089–1098.
2. Shen, H., & Zhao, L. (2013). ALERT: An anonymous location-based efficient routing protocol in MANETs. *IEEE Transactions On Mobile Computing*, *12*(6), 1079–1093.
3. Abbas, S., Merabti, M., Llewellyn-Jones, D., & Kifayat, K. (2013). Lightweight Sybil attack detection in MANETs. *IEEE Systems Journal*, *7*(2), 236–248.
4. Reina, D. G., Toral, S. L., Jonhson, P., & Barrero, F. (2011). A reliable route selection scheme based on caution zone and nodes' arrival angle. *IEEE Communications Letters*, *15*(11), 1252–1255.
5. Vergados, Dimitrios D., & Stergiou, Giannis. (2007). An authentication scheme for ad-hoc networks using threshold secret sharing. *Wireless Personal Communications, 43*, 1767–1780.
6. Bu, S., Yu, F. R., Liu, X. P., Mason, P., & Tang, H. (2011). Distributed combined authentication and intrusion detection with data fusion in high-security mobile ad hoc networks. *IEEE Transactions on Vehicular Technology*, *60*(3), 1025–1036.
7. Dahshan, H., & Irvine, J. (2009). On demand self-organized public key management for mobile ad hoc networks. In: *IEEE 69th Vehicular technology conference (VTC)*, Spring 2009, Barcelona.
8. Boppana, R. V., & Su, X. (2011). On the effectiveness of monitoring for intrusion detection in mobile ad hoc networks. *IEEE Transactions on Mobile Computing*, *10*(8), 1162–1174.
9. Li, L.-C., & Liu, R.-S. (2010). Securing cluster-based ad hoc networks with distributed authorities. *IEEE Transactions on Wireless Communications*, *9*(10), 3072–3081.
10. Ayday, E., & Fekri, F. (2012). An iterative algorithm for trust management and adversary detection for delay-tolerant networks. *IEEE Transactions on Mobile Computing*, *11*(9), 1514–1531.
11. Shanthi, N., Ganesan, L., & Ramar, K. (2009). Study of different attacks on multicast mobile ad hoc network. *Journal of Theoretical and Applied Information Technology, 6*(4), 45–51.
12. Palanisamy, V., & Annadurai, P. (2009). Impact of rushing attack on multicast in mobile ad hoc network. *International Journal of Computer Science and Information Security*, *4*(1&2)
13. Rangara, R. R., Jaipuria, R. S., Yenugwar, G. N., & Jawandhiya, P. M. (2010). Intelligent secure routing model for MANET. *Computer Science and Information Technology (ICCSIT), 2010 3rd IEEE international conference on Chengdu* (Vol. 3), July 9–11, 2010.
14. Rajan, C., & Shanthi, N. (2013). Misbehaving attack mitigation technique for multicast security in mobile ad hoc networks (MANET). *Journal of Theoretical and Applied Information Technology*, *48*(3), 1349–1357.
15. Khalil, I., & Bagchi, S. (2011). Stealthy attacks in wireless ad hoc networks: Detection and countermeasure. *IEEE Transactions on Mobile Computing*, *10*(8), 1096–1112.
16. van der Merwe, J., Dawoud, D., & McDonald, S. (2007). A survey on peer-to-peer key management for mobile ad hoc networks. *ACM Computing Surveys (CSUR)*, *39*(1). doi:10.1145/1216370.1216371.
17. EI Defrawy, K., & Tsudik, G. (2011). ALARM: Anonymous location-aided routing in suspicious MANETs. *IEEE Transactions on Mobile Computing, 10*(9), 1345–1358.
18. Tsudik, G., & Xu, S. (2006). A flexible framework for secret handshakes. In: *Proceedings of the privacy-enhancing technologies (PETs'06)*.
19. Ateniese, G., & Tsudik, G. (1999). Some open issues and new directions in group signatures. In: *Proceedings of the third international conference on financial cryptography* (pp. 196–211). Springer.
20. Lysyanskaya, A., Micali, S., Reyzin, L., & Shacham, H. (2004). Sequential aggregate signatures from trapdoor permutations. In: *Proceedings of the advances in cryptology (EUROCRYPT'04)* (pp. 74–90).
21. Khalil, I., & Bagchi, S. (2011). Stealthy attacks in wireless ad hoc networks: Detection and countermeasure. *IEEE Transactions on Mobile Computing*, *10*(8), 1096–1112.
22. Youssef, M., et al. (2014). Routing metrics of cognitive radio networks: A survey. *IEEE Communications Surveys and Tutorials, 16*(1), 92–109.
23. Attar, Alireza, et al. (2012). A survey of security challenges in cognitive radio networks: Solutions and future research directions. *Proceedings of the IEEE, 100*(12), 3172–3186.
24. Li, P., et al. (2012). CodePipe: An opportunistic feeding and routing protocol for reliable multicast with pipelined network coding. In: *INFOCOM 2012* (pp. 100–108).
25. Li, Peng, et al. (2014). Reliable multicast with pipelined network coding using opportunistic feeding and routing. *IEEE Transactions on Parallel and Distributed Systems, 25*(12), 3264–3273.
26. Zeng, Yuanyuan, et al. (2013). Directional routing and scheduling for green vehicular delay tolerant networks. *Wireless Networks, 19*(2), 161–173.
27. Busch, Costas, et al. (2012). Approximating congestion + dilation in networks via "quality of routing" games. *IEEE Transactions on Computers, 61*(9), 1270–1283.
28. Yen, Yun-Sheng, et al. (2011). Flooding-limited and multi-constrained QoS multicast routing based on the genetic algorithm for MANETs. *Mathematical and Computer Modelling, 53*(11–12), 2238–2250.
29. Meng, Tong, et al. (2015). Spatial reusability-aware routing in multi-hop wireless networks. *IEEE Transactions on Mobile Computing*. doi:10.1109/TC.2015.2417543.
30. Dvir, A., et al. (2011). Backpressure-based routing protocol for DTNs ACM SIGCOMM. *Computer Communication Review, 41*(4), 405–406.
31. Zhang, Xin Ming, et al. (2015). Interference-based topology control algorithm for delay-constrained mobile ad hoc networks. *IEEE Transactions on Mobile Computing, 14*(4), 742–754.
32. Vasilakos, A., et al. (2012). *Delay tolerant networks: Protocols and applications*. London: CRC Press.
33. Vasilakos, Athanasios V., et al. (2015). Information centric network: Research challenges and opportunities. *Journal of Network and Computer Applications, 52*, 1–10.

34. Yao, Guang, et al. (2015). Passive IP traceback: Disclosing the locations of IP spoofers from path backscatter. *IEEE Transactions on Information Forensics and Security, 10*(3), 471–484.
35. Yan, Zheng, et al. (2014). A survey on trust management for internet of things. *Journal of Network and Computer Applications, 42*, 120–134.
36. Yang, Haomin, et al. (2014). Provably secure three-party authenticated key agreement protocol using smart cards. *Computer Networks, 58*, 29–38.
37. Liu, Bingyang, et al. (2014). Toward incentivizing anti-spoofing deployment. *IEEE Transactions on Information Forensics and Security, 9*(3), 436–450.
38. Jing, Qi, et al. (2014). Security of the internet of things: Perspectives and challenges. *Wireless Networks, 20*(8), 2481–2501.
39. Zhou, Jun, et al. (2015). 4S: A secure and privacy-preserving key management scheme for cloud-assisted wireless body area network in m-healthcare social networks. *Information Sciences, 314*, 255–276.
40. Fadlullah, Z. M., et al. (2010). DTRAB: Combating against attacks on encrypted protocols through traffic-feature analysis. *IEEE/ACM Transactions on Networking's, 18*(4), 1234–1247.
41. Wang, Tao, et al. (2015). Survey on channel reciprocity based key establishment techniques for wireless systems. *Wireless Networks, 21*(6), 1835–1846.
42. He, Daojing, et al. (2012). ReTrust: Attack-resistant and lightweight trust management for medical sensor networks. *IEEE Transactions on Information Technology in Biomedicine, 16*(4), 623–632.
43. Zhou, Jun, et al. (2015). Secure and privacy preserving protocol for cloud-based vehicular DTNs. *IEEE Transactions on Information Forensics and Security, 10*(6), 1299–1314.
44. Yao, Guang, et al. (2015). Passive IP traceback: Disclosing the locations of IP spoofers from path backscatter. *IEEE Transactions on Information Forensics and Security, 10*(3), 471–484.
45. Yan, Z., et al. (2015). A security and trust framework for virtualized networks and software-defined networking. *Security and Communication Networks.* doi:10.1002/sec.1243.
46. Yang, Haomin, et al. (2014). Provably secure three-party authenticated key agreement protocol using smart cards. *Computer Networks, 58*, 29–38.
47. Zhou, Liang, et al. (2011). Joint forensics-scheduling strategy for delay-sensitive multimedia applications over heterogeneous networks. *IEEE Journal on Selected Areas in Communications, 29*(7), 1358–1367.

Prof. S. Vadhana Kumari received A.M.I.E. degree in Computer Science and Engineering from Institute of Engineers, Kolkatta, India. She obtained her M.E. degree in Computer Science and Engineering under Anna University. She is doing her Ph.D. in Anna University, the area of research is Security in MANETs. Currently She is working as an Assistant Professor and Head in Department of Computer Science and Engineering, in Maria College of Engineering and Technology, Attoor, Kanyakumari, Tamilnadu, India

Dr. B. Paramasivan received the B.E. degree from Madurai Kamaraj University, Madurai, Tamilnadu, India, in 1988, the M.E. degree from Jadavpur University, Calcutta, West Bengal, India, India, in 1994, and the Ph.D. degree from Anna University, Chennai, Tamilnadu, India, in 2009. He is currently working as a professor and head in the Department of Computer Science and Engineering, National Engineering College, Kovilpatti, Tamilnadu, India. His research interests are in quality of service for wireless networks. He is a reviewer of the IEEE Sensors Journal, Computing and Informatics Journal and Computer Networks and Communications. He is a senior member of the IEEE. He is a chairman of Information Theory Soceity. He has life membership of CSI Mumbai, ISTE New Delhi and a Fellow of Institution of Engineers (IE), Kolkatta. He serves as TPC member in various conferences, including the IEEE International Conference on Wireless and Optical Communications.