

Secured Self Organizing Network Architecture in Wireless Personal Networks

Pondi Jyothirmai¹ · Jennifer. S. Raj¹ · S. Smys²

Published online: 30 May 2017
© Springer Science+Business Media New York 2017

Abstract Secured self organizing network is an approach to computer network architecture that seeks to address the technical issues in heterogeneous networks that may lack continuous network connectivity. In delay tolerant network packets storage exists when there is any link breakage between the nodes in the network so delay is tolerable in this type of network during the data transmission. But this delay is not tolerable in wireless network for voice packet transmission. This evokes the use of wireless networks. In a network, different wireless network topologies are interoperating with each other so the communication across the network is called overlay network. This network is vulnerable to attacks due to mobile behaviour of nodes and frequent changes in topologies of the network. The attacks are wormhole attack and blackhole attack is analysed in this paper. They are critical threats to normal operation in wireless networks which results in the degradation of the network performance. The proposed recovery algorithm for wormhole and the isolation of blackhole will increase the performance of the network. The performance metrics such as throughput, packet delivery ratio, end–end delay and routing overhead of the network are evaluated.

Keywords Network attacks · Wireless security · Personal networks · Quality of service

1 Introduction

Communication in wireless networks are susceptible to different kinds of attacks due to the insecure channels. Communication remains a challenging and critical issue in wireless network. The main threats that oppose the security criteria, which are mainly known as security attacks. Two types of security attacks [1, 2], that are present in the network: passive attacks and active attacks [3]. In passive attack, the attacker monitors the

✉ S. Smys
smys375@gmail.com

¹ Department of ECE, Karunya University, Coimbatore, India

² Department of CSE, RVS Technical Campus, Coimbatore, India

transmission of data between the two parties or eavesdrops the data in the network. They do not desire to modify the content of the actual information. It does not change the data, so it is very difficult to detect. Passive attacks are of two types: release of message contents and traffic analysis. Active attacks [1] try to alter the system resources or affect their operation i.e. modification of the data stream or creation of a false stream. It consists of four categories. They are masquerade, replay, modification of message, and denial of service. Active attacks can be easily detected but passive cannot.

More-over attacker needs more time to get information about the target in passive attack but active attacker uses these information to launch a successful attack on target. The three goals of security [1] are confidentiality, integrity, and availability can be threatened by security attacks. Some of the active attacks are wormhole, blackhole, sinkhole, spoofing replay, denial of service, man in-middle attack etc. In this paper wormhole and blackhole attacks are analysed. Wormhole attack [4, 5] and blackhole attack [6] which comes under the network layer attacks [7, 8]. The wormhole attack can be identified by using forbidden topology technique [4]. The rest of this paper is organized as follows: section II describes related works that detect and prevents the wormhole attack in wireless networks. Section III describes wormhole attack & blackhole attack, section IV describes the proposed network scenario, section V describes verifier selection, network recovery process and isolation process followed by section VI presents simulation results and section VII describes conclusion.

2 Related Work

In [9], connectivity information is used for the detection of wormhole attack. However, these methods are not very effective when the networks become sparse because not enough connectivity information exists in the network. In [10], a general mechanism, called packet leashes, was presented for detecting and thus defending against wormhole attacks, and a particular protocol, called TIK was presented, that implements leashes. Authors introduced the general mechanism of packet leashes to detect wormhole attacks, and also presented two types of leashes: geographic leashes and temporal leashes. An efficient authentication protocol was designed by the authors, called TIK, for use with temporal leashes. Thus, in providing for wormhole detection, used an efficient symmetric cryptography, instead of relying on expensive asymmetric cryptographic operations. Keys in our protocol TIK are public values (once disclosed), although TIK uses only symmetric (not asymmetric) cryptography.

In [11], authors proposed an anti blackhole mechanism scheme. Drawback of this scheme is, appropriate security mechanism is required to have secured communication between the special IDS nodes. The performance of special IDS becomes more complex. In [12], explains the effect of blackhole attack and its variation in DTN routing. Authors proposed a ticket-based encounter prediction scheme to protect the DTN from blackhole attack. Whereas prediction is done based on contact history of the node. To secure the evidence of every contact and to avoid the adversary nodes from transfer of forge contact data it is essential to provide security in DTN. Blackhole attackers can reduce more packet delivery rate in DTN's absence of mandating encounter tickets based scheme. By using the encounter ticket scheme the number of packets that are dropped by the adversary became less. In [13], many research have been done to progress the security in mobile adhoc networks. In which most of them are depend on the cryptographic based techniques. But these techniques cannot prevent the adversary node from dropping the packets. Drawbacks are, proposed solution consists number of assumptions which is tough to recognize in a hostile environment like mobile adhoc networks are not always available due to deployment of the network limitations and cryptographic based computations are costly.

3 Attacks in Wireless Network

3.1 Wormhole Attack

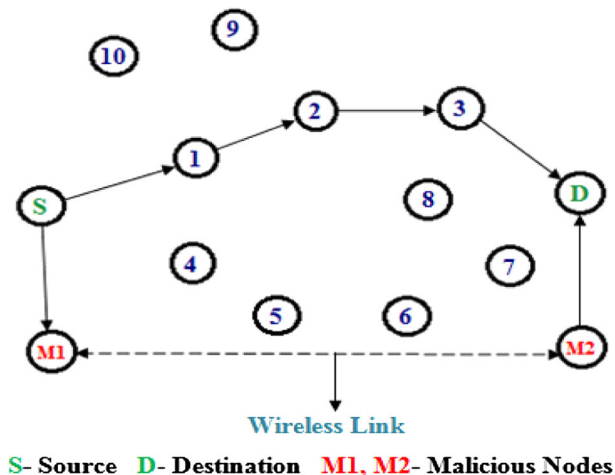
In wireless network the attacker can easily compromise the nodes. Wireless network will not work well in some challenging network scenarios as end-to-end path may not exist always. So attacker uses the compromised nodes in the network to launch a particular attack called wormhole attack. Wormhole attack is also known as tunnelling attack. Figure 1 shows that the network consists of two compromised nodes i.e. M1, M2, source S, destination D and nodes from one to ten are the normal nodes. Source "S" sends route request to the destination node "D". Then one compromised node i.e. M1 records the data and tunnels route requested data to another compromised node M2 which is present at the other end and replays them in network which is a neighbour of D. The destination node D gets two route request i.e. from the malicious node wireless link and other from the normal nodes as shown in Fig. 1. The route that results from the wormhole have lower hop count than normal routes. The number of hops between the two compromised nodes can be increased or decreased.

In case one, when hops are increases, the network think that they are far away from each other but actually they are nearer to each other. In case two, when hops are decreased, the network think that the compromised nodes are nearer to each other, but actually they may be far away. The outcome of making such wormhole links, the attacker can disrupt the routing in network as well it will corrupt the topology views of the network which it is attacked. The performance of the network significantly decreases due to the packet drop.

3.2 Effect of Blackhole Node in Manets

In AODV without attack in the network, when source wants to transmit packets to the destination, it will send route request (RREQ) to its neighbours to find the optimum path to the destination node in the network. After source receiving the multiple route response (RREP) consists of sequence number from the neighbour nodes, it decides the node which has greatest sequence one as the most recent fresh routing information and selects the route present in that RREP packet. Then it starts transmitting the packets to that node and discard all other responses from other neighbours. In Fig. 2. illustrate the blackhole attack, wherein the source node S i.e.

Fig. 1 Wormhole attack in wireless network



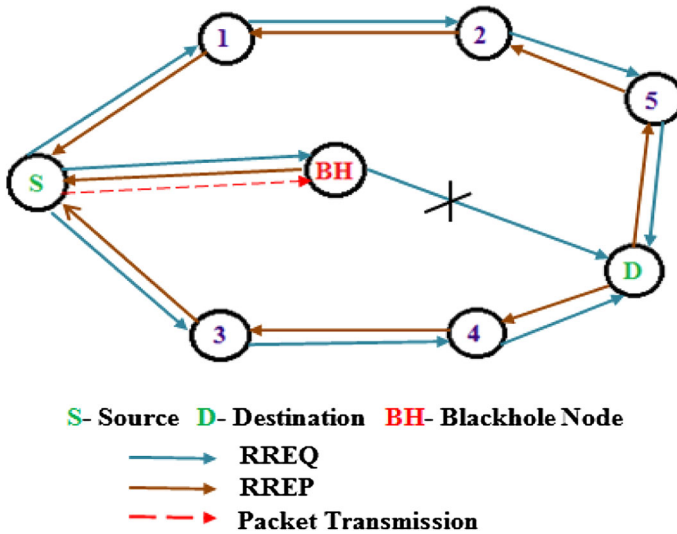


Fig. 2 Blackhole attack in wireless network

one of the verifier in the network topology is intend to establish a route to destination node D, by propagating route request (RREQ) packet. However, when blackhole node (BH) receives an RREQ from the source node, it sends an instantaneous fake RREP packet that means it shows that it is having the highest sequence number to a source node that starts the route discovery to impersonate to be a destination node. On receipt of an RREP from blackhole node, source starts sending the packets to the BH and discards all other responses.

The behaviour of black hole attack in the network can be of two types. In first case, the blackhole node captures packets from the source by showing the forged information to the source, it will drop more number of packets and sends only very few packets to the destination node. In second case, black hole node may fully drops the packets that are captured from the source node. Sometimes the black hole node capture all packets from the source node and it may not drop the packets. It may use those packets to launch dangerous threat in the network. The network overhead increases due to black hole attack, degrades the network's lifetime by boosting energy consumption, and finally destroys the network. Thus makes this type of attack is more dangerous as it does not check what kind of data just dropping the packets is meant for other nodes. That data may be critical. So this type of attack must be detected as early as possible and removed from network.

4 Proposed Network Scenario

The wireless network scenario consists of different network topologies. The topologies considered are star topology, mesh topology, ring topology and bus topology. They interoperate each other by exchanging the information in the network. Communication across the network is called an overlay network. Overlay network that links together multiple subnets into a single network. Figure 3 explains the architecture construction for overlay network without and with attack. Each topology consists of two fixed verifiers as shown in Fig. 3a which verifies the network, a source (V_1) and destination (V_2). The verifiers in the network have the transmission range of 250 m.

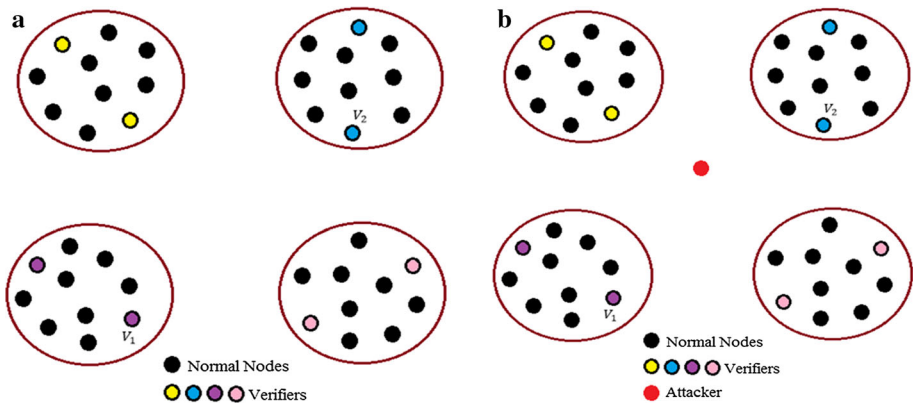


Fig. 3 Interoperable architecture construction for overlay network. **a** Example of selection of verifiers and **b** wireless network with attack

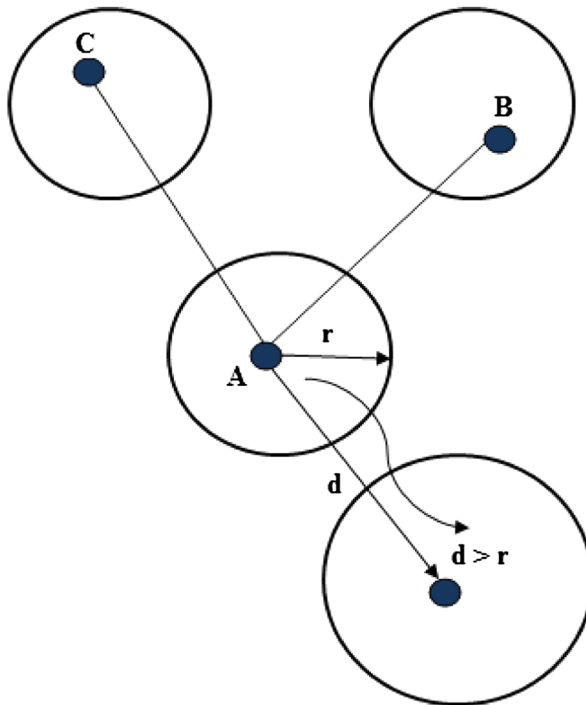
The nodes in different topologies are connected in a triangulation model [4] and interoperate each other by allowing the information exchange. The tree structure called Kruskal's algorithm [14], that finds a shortest spanning tree for a connected weighted undirected graph is used to form links from the verifier to the other nodes in the network. The verifier calculates the distance between the nodes which are present in its transmission range. This distance can be calculated by using the Euclidean distance [15] method. The advantage of using more verifiers in different network topologies will minimize the computational time and complexity in each topology. Wireless networks are vulnerable to wormhole attacks due to the mobility of nodes when different network topologies are interoperating each other as shown in Fig. 3b. It can be detected by using the forbidden topology technique [3] which examine the node location under the limitation of transmission range. In the recovery process of the wormhole attack and isolating the blackhole attack, after identifying the malicious node in the network by the verifier node, it will inform to all the verifiers in the network, not to communicate with that particular node. Therefore the malicious node is not considered in the network as a result network becomes secure and the performance of the network will increases.

5 Verifier Selection

5.1 Theorem

A node in a network can take the place of a backbone which is a verifier node, only when its power is high and less failure.

Proof Consider some fixed nodes which act as a backbone of a network in each individual network topology. Suppose A, B, C are the backbone nodes having the transmission range R . The node is selected which has high power and less failure. The backbone node consists of connected dominant set (CDS). When backbone has to move, it will hand over the role to the neighbour nodes. The neighbours are, node whose distance d is less than the transmission range r i.e. $d < r$, and whose node power is high will be the next backbone. Figure 4 shows, if verifier wants to moves other location if its distance d is greater than r i.e. $d > r$, then it will form a new connected dominant set which are located in its transmission range.



A,B,C - Backbone Nodes **r** - Radius **d** - Distance

Fig. 4 Node as backbone

5.2 Algorithm I: Identifying Wormhole Attack

1. **forall** $X_i \in N$ **do**
2. **if** $V_{tr} = 250$
3. **then** $L_{V_n} \leftarrow A, B, C$ and
4. **if** $V_{tr} = V_{tr}/2$
5. **then** $B, C \notin L_{V_n}$ and $A \in L_{V_n}$
6. puts "A is attacker"

where $X_i = \{A, B, C\}$, V_{tr} = transmission range of the verifier, L_{V_n} = list of verifier neighbours, N = nodes in a network

5.3 Algorithm II: Recovery Process

1. **forall** $X_i \in N_V$ **do**
2. **if** $X_i \in V_m$
3. **then** discard the node and
4. **also** $V_m \rightarrow o_V$

where V = verifier, N_V = nodes of V , V_m = malicious nodes list of V , o_V = Other verifier nodes in the network

5.4 Algorithm III

```

// Detection and Isolation of the Blackhole Attackers
Input:
// Initialize the number of nodes in the network topology
// Selection of verifier nodes
// Initialization of the neighbour list in the routing table present in its transmission range
Step 1: Sending the route request to find the optimum path
Step 2: Verifier  $V_1$  having the routing table, which maintains all the route response from its neighbour
nodes having its sequence number
Step 3: Check for the neighbour with highest sequence number
    If true then
        // send ( )
    Else
        // discard ( )
Step 4: // Presence of Attacker
    // Interpretation of wrong info ( )
    info ( )
    {
        // Intimating highest sequence number and getting packets
    }
Step 5: // Detection of Attacker
    If range = yes then
    {
        // gives its response
    }
    Else
    {
        Compromising the nodes // by shortest distance
    }
Step 6: All attacker nodes in the network will be updated into suspected list
Step 7: // Isolation of Attacker
    If (seqno > 100)
    {
        Node = attacker
    }
    Else
    {
        Normal node
    }
Step 8: // Selection of alternative path
Step 9: Repeat step 7
Step 10: // Broadcasting of the attacker nodes to other verifiers in network
Output: Detection and isolation of attacker nodes in the network

```

As shown in Fig. 3b. Verifier V_1 can detect the attacker in two ways. In first case, attacker that is not present in the transmission range of the verifier V_1 but advertises by itself it is the neighbour to it by compromising the nodes that it having the shortest path to V_2 and sends response that it having highest sequence number. Second case, attacker node that is present in transmission range and sends false information to the V_1 .

Verifier V_1 node having the routing table which maintains all the responses from its neighbours having the sequence number All the sequence number of the route response packet is compared by the verifier V_1 node. The sequence number of the normal node is incremented by 2 each time. The maximum sequence number for the normal network without attack is 50. But the attacker node shows the forge sequence number which is greater than the normal node sequence number with much difference.

The threshold value taken is 100. If the sequence number of a node is more than the 100, then that node is consider as an attacker node and updated into the suspected list. This list is informed to all other verifier nodes in the network. Now, when verifier V_1 wants to communicate with the destination V_2 i.e. another verifier node in different network topology, if the nodes in the suspected list falls into this path then verifier V_1 selects alternative path to the destination and again compares the sequence number of that particular node. As a results data transmission to the attacker node is stopped and packets are delivered to the destination. So, the packet drop ratio decreases and overall performance of the network will be increases.

If the sequence number is genuine, then source V_1 starts data transmission to the destination node without any packets or information loss. This solution, by isolation of black hole attack will keep the network secure. As a result data transmission will happen in a proper manner. The advantage of this method, it is useful even when more number of attackers present in the network as well as when attackers are cooperative. Cooperative attackers can be identified by frequent communication between that nodes which means received packets will be more than the number of sent packets.

6 Simulation Results

The tool used to perform the process is network simulator NS-2 and NS-3 software [16]. The implementation of the protocol has been done using C++ language in the backend and Tcl language in the frontend on the Ubuntu Linux 10.4 operating system using ns-2 and only C++ language is used in case of ns-3. The simulation parameters for analysis is

Table 1 Simulation parameters

Simulator	NS-2 and NS-3
Number of nodes	100
Routing protocol	AODV
Number of blackhole nodes	3
Packet size	512 Bytes
Region covered	3000 × 3000
Traffic type	TCP-FTP and UDP-CBR
Mobility model	Random Waypoint Propagation Model
Bandwidth	2 Mbps
Simulation time	100 s
Transmission range	250 m

provided in Table 1. The channel used is wireless channel with two ray ground radio propagation model and the size of the packet is 512bytes. The routing protocol used for analysis is AODV routing protocol. Nodes in the network are created randomly and number of nodes considered are 100 nodes. Simulation time is 100 s. The metrics used to evaluate the performance are given below.

6.1 Performance Metrics Evaluated

The performance metrics such as throughput, packet delivery ratio, end–end delay, routing overhead and goodput are computed. These parameters are computed with the data present in the trace file. These parameters helps to analyse the performance of the network.

Throughput Throughput is defined as the ratio of successfully received packets to generated packets per unit time. The unit of throughput is Kbits per second.

Packet delivery ratio (PDR) PDR is defined as the ratio of total number of received packets by the destination to the total number of transmitted packets at the source. PDR is calculated in terms of percentage.

End–end delay End–End Delay is calculated as ratio of total delay to total packet count. Its unit is in time.

Routing overhead Routing overhead is defined as the ratio of number of control packets generated and the number of data packets received by the destination. Its unit is Kbps.

Goodput Goodput is defined as a ratio of amount of data received by the receiver per unit time. Its unit is bits per second.

6.2 Performance Analysis of Wormhole Attack

Figure 5a shows the throughput performance of node in the ring topology. Throughput value is 5500bps with a simulation time period at 36 s because the network is not attacked by the malicious node during that period, so throughput is high. Initially the packet transmission starts from 9 s and the throughput performance value is 4000 bps because of the malicious node. Due to packets drop throughput performance of the network is degraded to a value of 1200 bps at 100 s.

Figure 5b illustrates the throughput performance of a node in the mesh topology. In normal situation network without any attack, the throughput performance of a network is high i.e. 3800 bps at 9 s. But gradually the throughput value is degraded to a value of 200 bps at 100 s due to the effect of malicious node, packets in the network are dropped. Figure 5c explains the throughput performance of bus topology, the network is attacked by the malicious node as a result the throughput performance initially is low i.e. 3500 bps at simulation time of 9 s and degradation continued up to 66 s that can be observed between 10 s and 73 s. But the throughput performance is high i.e. 15,000 bps at 73 s because the network is not attacked during this time period. The throughput performance of the star topology is shown in Fig. 5d due to the presence of attack throughput is reduced from 6000 bps at simulation time of 15 ms to 2500 bps at 100 s. The performance is significantly reduced because of packet drop.

The throughput performance of the overall network, when different network topologies are interoperating each other is shown in Fig. 6. After identifying the malicious node in the network they will not be considered by the verifier node. That nodes will be discarded. The

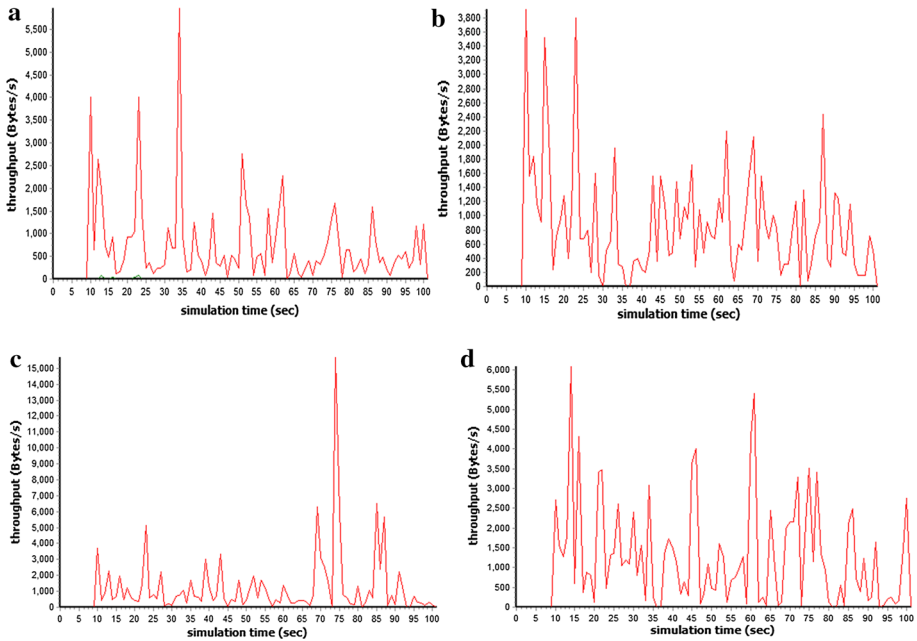
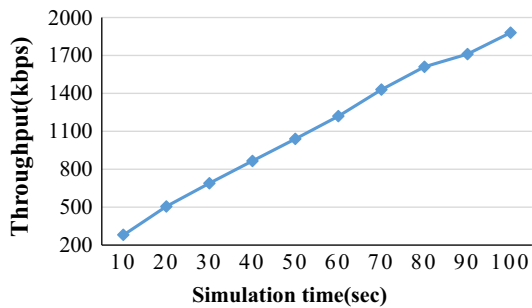


Fig. 5 Throughput graphs. **a** Throughput in ring topology. **b** Throughput in mesh topology. **c** Throughput in bus topology. **d** Throughput in star topology

Fig. 6 Recovered throughput performance of an overall networks



performance increased from 10 to 100 s to a value of 85.106%. Figure 7 illustrates the end-end delay over the time in the network is initially less and delay is increased to 7.5 ms when network is attacked by the malicious node. Then after identifying the malicious node the delay is reduced to 0.5 ms. Table 2 illustrates the packet delivery ratio of the network with and without presence of attacker also its isolation is analysed. The performance of the network topology increased from 67 to 86% after the recovery process.

6.3 Performance Analysis of Blackhole Attack

Figure 8 shows, the network with and without malicious nodes and its impact on throughput by varying the number of nodes and number of malicious nodes. Throughput performance of the network without attack is reduced as the number of nodes are increased

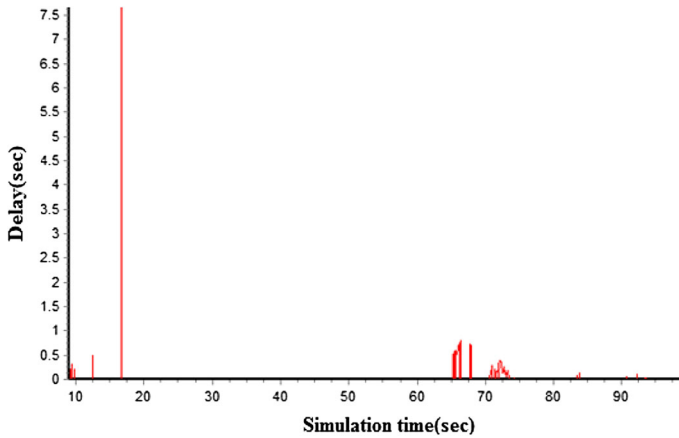
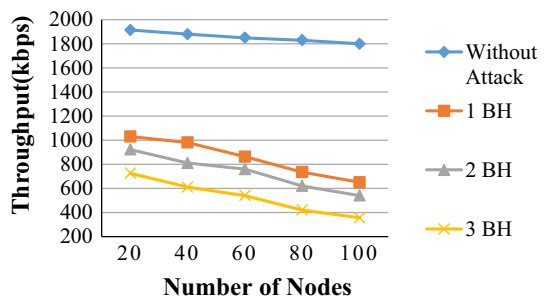


Fig. 7 Recovered end-end delay in the network

Table 2 Packet delivery ratio with attack and recovery of network from attack

Number of malicious nodes	Network	Packet delivery ratio (%)
0	Without attack	98
2	With attack	67
2	Recovery	86

Fig. 8 Throughput performance with attack



because the distance between the source and destination nodes increases also due to the increment of intermediate nodes on the path. When the network is attacked by the malicious node the throughput performance of the network is diminished more when compared with the network without blackhole attack due to the dropping of packets by the attacker node during the data transfer. It also shows that, decrement in network throughput even more with the increase in number of blackhole nodes. Network in the absence of attack throughput performance is 1914 kbps, with malicious the throughput is reduced to 356 kbps.

Figure 9 shows, the network with and without malicious nodes and its consequences on packet delivery ratio by varying the number of nodes and number of malicious nodes. As the number of nodes in the network increases packet delivery ratio of AODV protocol

diminishes due to increase in the number of intermediate nodes on a path and distance between source and destination on the route. The packet delivery ratio of the network with attack diminishes even more because the blackhole node will become an intermediate node on the path between source and destination node in network topology. In the absence of attack, packet delivery ratio is 98.932%, with attacker node the packet delivery ratio in the network is reduced to 55.16%.

Figure 10 shows the effect of blackhole nodes on end–end delay in the network scenario. Time taken to process and transmit the packets without attack is less between source and destination node compared with the attacker in the network because number of packets processed is less. In Ad hoc On-Demand Distance Vector routing protocol, end to end delay in the network increased with increase in number of blackhole nodes in the presence of blackhole nodes because time needed to process and transmit the packets to the destination node takes much time by the blackhole nodes in the network topologies. The delay value without attack is 0.432 s and is increased by 16 s with the blackhole nodes in the network. Figure 11 illustrates the throughput performance of the network after isolation of black hole attack by varying the number of nodes and the number of attackers. Therefore after isolating the blackhole in the network the throughput performance is increased due to decrease in packet drop by the blackhole node. Without attack throughput is 1914 kbps and network with blackhole node the throughput performance is reduced to 356 kbps and after isolating the black hole attack in the network the throughput is increased to 1654 kbps.

Figure 12 explains, the performance of the packet delivery ratio after isolation of black hole attack. In the absence of blackhole nodes in the network, AODV protocol performs much better and simple. There is no security mechanism present in ad hoc on demand distance vector protocol to protect and overcome the adversary attacks. So very few of the data packets reach the destination node in the network topology. The source node or other nodes in the network discards RREP packets coming from blackhole nodes and hence does

Fig. 9 Packet delivery ratio with attack

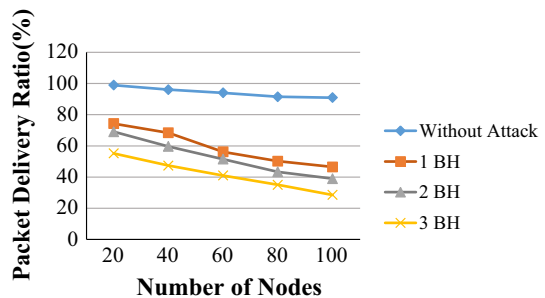


Fig. 10 End–end delay with attack

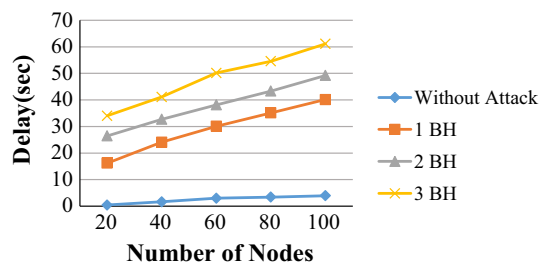


Fig. 11 Throughput after isolation of blackhole attack

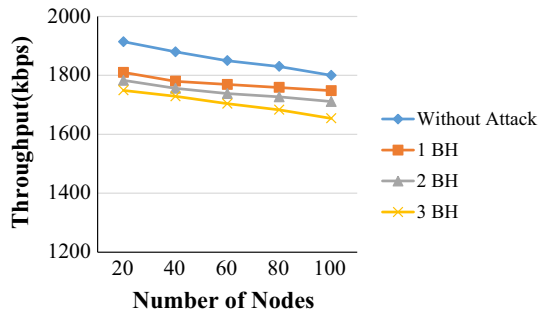
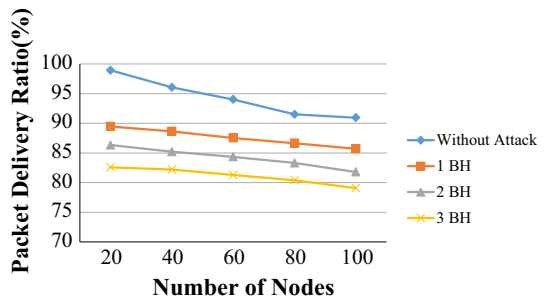


Fig. 12 Packet delivery ratio after isolation of blackhole

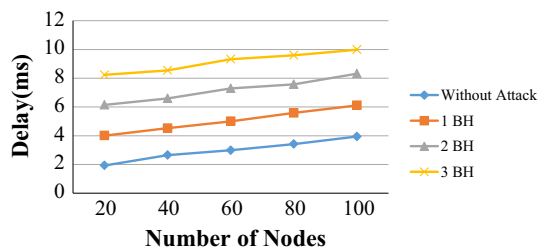


not establish route through blackhole node. Therefore, packet delivery ratio of the network increases after isolation of the black hole attack when number of attacker nodes is incremented. Packet delivery ratio after isolating the black hole attack is incremented from 55.16 to 83.08%.

Figure 13 illustrates the performance of end-end delay after isolation of black hole attack by varying the number of nodes and blackhole nodes. Delay of the network is decreased after isolation of the network because processing time of the data packet is less between source and destination. Even the attacker sends immediate response to the request that sent by the source node when compare with the other nodes in the network, the source node will not establish any path to the destination as a result the delay of the network is reduced compared network with attack. Delay of the network is reduced from 16.231 to 4.01 ms after isolation of black hole attack.

Figure 14 explains, routing overhead with & without black hole attack by varying the number of nodes and number of blackhole nodes. Absence of attack, the network consists of overhead because due to mobile behaviour of nodes, the failure of the links between the source and destination and retransmissions of packets increases the load in the network etc.

Fig. 13 End-end delay after isolation of blackhole



In case one, if every node in the network topologies maintains the routing table, it results in increment of network overhead also diminishes the performance of the network. In our scenario, verifiers in each network topology maintains routing table. In case two, black hole attack in the network increases overhead by increasing the number of nodes and blackhole nodes because they send forge replies to the requesting packets. As a result the behaviour of the protocol changes and transmits additional routing packets in the network. Routing overhead of the network, absence of attack is 198.54 kbps and with attack is 252.36 kbps. Figure 15 illustrates, routing overhead after isolation of black hole attack by varying the number of nodes and blackhole nodes in the network. The routing overhead increases after isolation of black hole when compared with the AODV protocol due to the verifying process involved to choose alternate and optimum path to the destination by avoiding attacker node while packet transmission from source to the destination. Routing overhead of the network is increased from 252.36 to 302.46 kbps after isolation of black hole in the network.

The behaviour of black hole attack in the network can be of two types. In first case, the black hole node captures packets from the source by showing the forged information to the source then drops more number of packets and sends only very few packets to the destination node. Case one is analysed using NS-2.35 environment. In case two, black hole node fully drops the packets that are captured from the source node in the network. Fully dropping of packets by the black hole node behaviour is analysed using NS-3 tool.

Table 3 clearly shows the performance of the network i.e. throughput and goodput with and without blackhole attack and its isolation are shown. In this table D, M indicates destination and blackhole node. Goodput of the network is lesser than the throughput because it contains only data packets whereas throughput consists of both control and data

Fig. 14 Routing overhead with and without blackhole attack

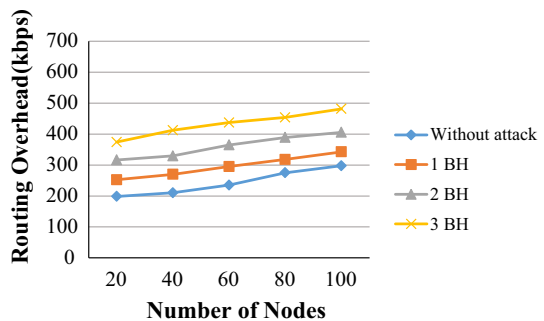
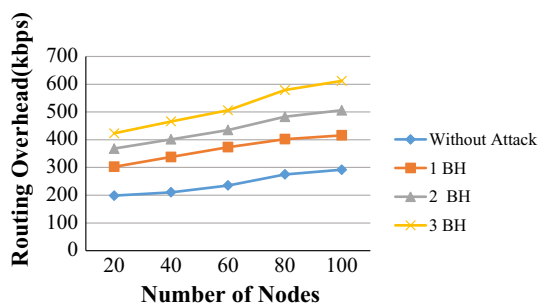


Fig. 15 Routing overhead after isolation of blackhole attack



packets. Throughput, goodput of the network absence of attack is 1856.03 and 1731.18 kbps.

With attack the performance of the destination node in the network is reduced due to blackhole node captures packets from source by showing fake data and drops all the packets, during the isolation throughput, goodput is increased compared with network in presence of attack. Throughput and goodput performance of a black hole node is 0kbps after isolation because packets are not fed to the black hole node once it is detected instead takes alternate path to the destination node.

Table 4 shows the overall throughput performance of the network with, without blackhole attack and its isolation is shown. Number of nodes considered in network scenario are 100 nodes. With attack the performance of the network is 0 Mbps that means the packets received by the black hole node are fully dropped. After isolation performance is increased to 1.728 Mbps and without attack is 1.947 Mbps.

Tables 5, 6 shows the overall good put and packet delivery ratio performance of the network with/without attack and its isolation are shown. With attack the goodput and packet delivery ratio performance of the network is 0 Mbps, without attack goodput is 1.713 Mbps and after isolation value obtained is 1.582 Mbps. Without attack the overall packet delivery ratio is 95.136% and after isolation the packet delivery ratio is 89.427%.

Table 7 shows the overall delay performance of the network. The end-end delay in the network is less when compared with tcp because no acknowledgement in case of udp. Overall delay after isolation is 1.037 s, without attack delay is 0.214 s. With attack delay is 7.562 s because of more processing time is needed with the black hole to reach packets to destination.

Table 3 Throughput and goodput of the destination, not black-hole/blackhole node

	Node	Throughput (Kbps)	Goodput (Kbps)
Without attack	D(27)	1856.03	1731.18
	Not M (35)	1798.84	1698.25
With attack	D(27)	0	0
	M (35)	1265.29	1048.07
Isolation	D (27)	1612.51	1593.16
	M (35)	0	0

Table 4 Overall throughput performance

Number of nodes	Network	Overall throughput (Mbps)
100	Without attack	1.947
	With attack	0
	Isolation	1.728

Table 5 Overall goodput performance

Number of nodes	Network	Overall goodput (Mbps)
100	Without attack	1.713
	With attack	0
	Isolation	1.582

Table 6 Overall packet delivery ratio performance

Number of nodes	Network	Overall packet delivery ratio (%)
100	Without attack	95.136
	With attack	0
	Isolation	89.427

Table 7 Overall end to end delay performance

Number of nodes	Network	Overall delay (s)
100	Without attack	0.214
	With attack	7.562
	Isolation	1.037

7 Conclusion

Wormhole and Black hole attack are main security threats that degrades the performance of routing protocol in Mobile Ad hoc Network. Its detection and isolation is the main factor of concern to improve network quality. Performance metrics such as packet delivery ratio, throughput, end–end delay, goodput and routing overhead are analysed by varying the number of nodes and blackhole nodes in the network. The throughput value of a network is reduced to 1030 kbps and below when blackhole nodes are increasing and increased the throughput performance to 1810 kbps by isolating the black hole attack. End–end delay is increased by 16 s with blackhole attack from 0.782 s without attack, after isolation of attack delay is reduced to 4.01 s. Packet delivery ratio is 98.392% without attack and decreased to 55.16% when the network is attacked by the attacker node after isolation it is increased to 83.08%. Routing overhead is 198.54kbps without attack in the network, with attack overhead is 252.36 kbps and increased to 302.46kbps after isolation. Therefore, the performance of the network is increased due to decrease in packet drop rate in the network and also multiple attackers can be detected. More than 80% of the performance of the network is increased after recovery and isolation of attacks in the wireless network. Future work implementation in the real time, by considering military fields, relief camps, hostile environments etc.

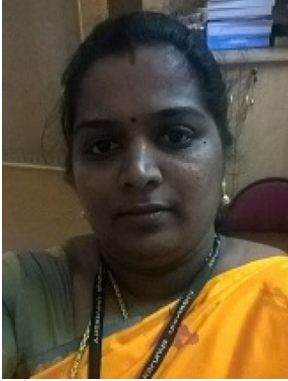
References

1. Wu, B., Chen, J., Wu, J., & Cardei, M. (2006). A survey on attacks and countermeasures in mobile adhoc networks. In Y. Xiao, X. Shen & D.-Z. Du (Eds.), *Wireless/mobile network security* (pp. 1–38). Berlin: Springer.
2. Supriya, K. M. (2012). Mobile Ad Hoc networks security attacks and secured routing protocols: A survey. In: N. Meghanathan, N. Chaki & D. Nagamalai (Eds.), *Advances in computer science and information technology. Networks and communications. CCSIT 2012. Lecture notes of the institute for computer sciences, Social informatics and telecommunications engineering* (Vol. 84, pp. 119–124). Berlin: Springer.
3. Liang, Y., Poor, H. V., & Ying, L. (2011). Secrecy throughput of MANETs under passive and active attacks. *IEEE Transactions On Information Theory*, 57(10), 6692–6702.

4. Ren, Y., Chuah, M. C., Yang, J., & Chen, Y. (2010). Detecting wormhole attacks in delay-tolerant networks [Security and Privacy in Emerging Wireless Networks]. *IEEE Wireless Communications*, 17(5), 36–42.
5. Hu, Y.-C., Perrig, A., & Johnson, D. B. (2006). Wormhole attacks in wireless networks. *IEEE Journal on Selected Areas in Communications*, 24(2), 370–380.
6. Tseng, F. H., Chou, L. D., & Chao, H. C. (2011). A survey of black hole attacks in wireless mobile ad hoc networks. *Human-centric Computing and Information Sciences*, 1(1), 4.
7. Ghonge, M. M., Jawandhiya, P. M., & Ali, M. S. (2011). Countermeasures of network layer attacks in MANET. In *IEEE conference special issue on network security and cryptography*.
8. Nadeem, A., & Howarth, M. P. (2013). A survey of MANET intrusion detection & prevention approaches for network layer attacks. *IEEE Communications Surveys & Tutorials*, 15(4), 2027–2045.
9. Maheshwari, R., Gao, J., & Das, S. R. (2007). Detecting wormhole attacks in wireless networks using connectivity information. In *Proceedings of IEEE INFOCOM*.
10. Hu, Y.-C., Perrig, A., & Johnson, D. B. (2003). Packet leashes: A defense against wormhole attacks in wireless networks. In *Proceedings of IEEE INFOCOM*.
11. Su, M.-Y. (2011). Prevention of selective black hole attacks on mobile ad hoc networks through intrusion detection systems. *Computer Communications*, 34, 107–117.
12. Li, F., Srinivasan, A., & Wu, J. (2009). Thwarting blackhole attacks in disruption-tolerant networks using encounter tickets. In *Proceedings of IEEE INFOCOM*.
13. Djahel, S., Nait-Abdesselam, F., & Zhang, Z. (2011). Mitigating packet dropping problem in mobile ad hoc networks: Proposals and challenges. *IEEE Communication Surveys*, 13(4), 658–672.
14. Guttoski, P. B., Sunye, M. S., & Silva, F. (2007). Kruskal's algorithm for query tree optimization. In *International database engineering and applications symposium*. IEEE.
15. Euclidean Distance. <http://www.pbarett.net/techpapers/euclid.pdf>, accessed. 29 March 2015.
16. Network Simulator 2 & 3. <http://www.isi.edu/nsnam/ns>.



Ms. Pondi Jyothirmai received her B. Tech. degree in Electronics and Communication Engineering at Jawaharlal Nehru Technological University Hyderabad, in 2013. Since July 2013, she has been a student of M. Tech. in Communication Systems at Karunya University, Coimbatore. Her research interest includes in wireless networks and topology control structures.



Dr. Jennifer S. Raj received the Ph.D. degree from Anna University and Masters Degree in communication System from SRM University, India. Currently she is working as an Assistant Professor, Department of ECE, Karunya University, Coimbatore, India. Her interests are in wireless networks with self organization and topology control structures. She is a life member of ISTE, India. She is book reviewer for Tata McGraw Hill publication and publishes more than fifteen research articles in the journals and IEEE conferences.



Dr. S. Smys received the Masters Degree in Digital Communication and Network Engineering from Anna University, India and completed Doctorate work in Wireless Networks from Karunya University, India. Currently he is working as a professor in Karpagam College of Engineering, Coimbatore, India. Also he is an associate editor of Elsevier Computers and Electrical Engineering Journal. His research interests are self organization and topology control in mobile networks. He also a reviewer for various Springer journals, IET Communication, Elsevier publications and various IEEE conferences and publish more than thirty five research articles in journals and international conferences.