Wireless Pers Commun (2016) 90:1039–1050
DOI 10.1007/s11277-016-3318-5

Localized Secure Routing Architecture Against Cooperative Black Hole Attack in Mobile Ad Hoc Networks

T. Poongodi[1] · **M. Karthikeyan**[2]

Published online: 16 April 2016

Abstract Black hole attack refers an attack by single or more number of malicious nodes which forcibly captures the route from source to destination by sending reply with largest sequence number and smallest hop count. In this paper, a novel technique using Localized Secure Architecture for MANET (LSAM) routing protocol is proposed to detect and prevent co-operative black hole attack. Security Monitoring Nodes (SMNs) would be activated only if the threshold value is exceeded. If malicious nodes are detected, other SMNs in its proximity area are intimated to isolate the malicious nodes. Network simulator tool is implemented to analyze the network performance of different scenarios with various number of nodes. Packet delivery ratio (PDR), routing overhead, control overhead, packet drop rate, throughput and end-to-end delay (EED) are the factors taken into consideration for performance analysis and it is shown that the proposed protocol is more secured and efficient. PDR is been increased by 27 % in the presence of 40 % misbehaving nodes, while it increases the percentage of overhead on proposed routing protocol from 1 to 4 %. EED is greatly reduced from 0.9 to 0.3 % in LSAM.

Keywords Ad hoc on-demand distance vector (AODV) · Packet delivery ratio · Routing overhead · Control overhead · Packet drop ratio · Throughput · End-to-end delay

✉ T. Poongodi
res.rcrr@gmail.com; tpoongodi2730@gmail.com

M. Karthikeyan
mkarthikn@rediffmail.com

[1] Department of Computer Science and Engineering, PPG Institute of Technology, Coimbatore, Tamilnadu, India

[2] Department of Electronics and Communication Engineering, Tamilnadu College of Engineering, Coimbatore, Tamilnadu, India

1 Introduction

Wireless mobile devices are extensively used in many application areas such as military services, disaster relief, networking communications, conferences etc. A Mobile Ad hoc NETwork (MANET) consists of wireless mobile nodes where each node acts as a host or router for forwarding and routing packets. In MANET, nodes within transmission range can communicate directly over radio links without any central coordinator. Due to its characteristics like open medium, dynamic topological configuration, it is more vulnerable to various types of attacks [1–3]. Moreover, MANET features make routing process very difficult when compared to infrastructure based wireless networks. Therefore, providing secure routing service with minimum overhead is a challenging task [4]. Hence, an optimal route has to be discovered which passes through many intermediate nodes in order to transfer packets from source node to destination node. The need for establishing an optimal efficient route is the main responsibility of dynamic routing protocols where the network topology changes dynamically. In MANET, routing protocols are categorized into proactive, reactive and hybrid protocols [5, 6]. Proactive routing protocol like Destination Sequenced Distance Vector (DSDV), Optimized Link State Routing (OLSR) obtains routing information by periodically exchanging topological information between nodes. But it has the disadvantage of continuous updation of routing entries. Reactive routing protocol such as in Dynamic Source Routing (DSR), Ad hoc On-demand Distance Vector (AODV) a route is established for a node only when there is a need.

AODV is an on-demand (reactive) routing protocol where the source node (N_S) needs to establish a connection with destination node (N_D); It initiates route discovery process by broadcasting Route REQuest (RREQ) packets to its neighboring nodes [7]. To launch the route, it must go through route discovery and route maintenance phase. In route discovery phase, AODV uses RREQ and Route REPly (RREP) messages to obtain a route. When any intermediate node receives RREQ message, it starts to communicate with the source node by unicasting RREP message. Once the source node has received RREP message, it is ready to transmit data packets to the destination node. In route maintenance phase, the source node is informed about the link failure by transmitting the Route ERRor (RERR) message.

2 Related Work

Routing misbehaviors are the major security threats in MANET. Intruders choose to compromise some nodes in ad hoc networks, and utilize those nodes to disturb the routing services of the entire network [8]. Intrusion Detection system is a solution to wide range of security attacks in MANET. It is used for only detecting attacks however it cannot prevent or respond. Once the intruder is detected, an alarm message can be sent to inform other nodes to take action. Various intrusion detection mechanisms operate with both proactive and reactive routing protocols. These mechanisms facilitate the network to identify and isolate the intruded nodes from it [9–12]. Using AODV, an intruder node falsely sends the RREP that it has the latest short route with minimum hop count to destination. After capturing the route, it drops all the receiving data packets. The authors proposed dynamic anomaly detection system based on dynamic learning process for enhancing security in MANET [13].

A context adaptive IDS system is proposed to detect potential security threats of a given node and examined new arriving packets. IDS nodes are positioned in a sniff mode in order to estimate the suspicious value of a node based on computing the difference between RREQ and RREP transmission time. If the suspicious value of a monitored node is

exceeding a threshold value, a block message is broadcasted to all nodes in the network for isolating the malicious node from the network cooperatively [14].

A black hole attack is an attack where the malicious node forcibly obtains the route with greatest sequence number and less hop count and subsequently overhears or drops all data packets. Figure 1 illustrates the behavior of black hole attack where a black hole is a node that behaves like a normal node; moreover it may be a single node or a cooperative node (i.e. existence of two malicious nodes). The source node S broadcasted RREQ packet to all neighboring nodes which in turn forwards to next node if it is not the destination node. Both the destination node D and the malicious node BH_1 sends RREP packet with largest sequence number and smallest hop count. Based on AODV protocol routing procedure, the source node S would prefer a shortest route of malicious node BH_1 because of its smallest hop count 1 [15, 16]. After obtaining the route, the malicious node overhears the upcoming packets or it may drop all packets which have been received. Cooperative black hole node BH_2 is being introduced to strengthen the malicious activities and also to reduce the chance of finding the existence of malicious node BH_1. Both malicious nodes BH_1 and BH_2 may partially overhear or drop the packets.

For secure transmission Digital Signature Algorithm (DSA) is followed, a fixed length message digest d is computed by passing through hash function H for every DP as $H(DP) = d$. Data packets are signed by the sender using its own private key and it is transmitted via unsecured channel. Receiver then computes the received data packets DP' against the decided hash function H to reveal the message digest d'. Then it is verified using sender's public key by the destination node $H(DP') = d'$. Similarly ACK packets are signed by the destination node $H(ACK) = d$ and verified by the source node $H(ACK') = d'$. DSA has been chosen due to its signature size and less network overhead. Moreover, routing overhead would be more if RSA scheme is chosen because of the existence of malicious nodes for signature creation and verification. Digital signature

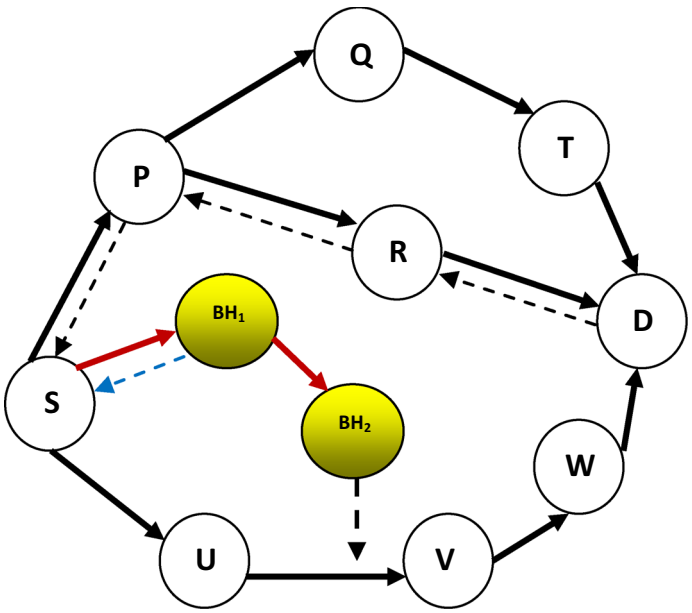

Fig. 1 Cooperative black hole attack

scheme is more desirable in MANET when compared to RSA scheme [17]. The simulation is conducted with co-operative black hole attack as a case study that concerns the most popular protocol AODV. The simulation results of the Network Simulator (NS-2) [18] demonstrate the effectiveness of LSAM in terms of packet delivery ratio (PDR), routing overhead (RO), control overhead (CO), packet drop rate (PDr), throughput (Th) and end-to-end delay (EED) with respect to various number of nodes.

3 Proposed Methodology

According to AODV protocol, the source node N_S finds the route by broadcasting RREQ for transmitting packets to the destination node N_D. If the path is available, the destination node or any other intermediate node sends reply to the source node by unicasting RREP. During the route discovery phase, the introduced malicious nodes acquire the route and it behaves like other normal nodes. As soon as the shortest path is identified, the source node initiates the transmission of data packets. The malicious nodes actively participate in the route discovery process and declare the route with greatest sequence number and less hop count. Malicious nodes behave like other normal nodes by unicasting the shortest route. The source node absolutely and unknowingly prefers the route which is proclaimed by the malicious node(s) through RREP packet. The shortest path calculation is based on the below equation.

$$Sp = \sum_{l \in N} w(l) \tag{1}$$

Here Sp denotes the shortest path and it depends on the w(l) weight of the link. This weight of the link is defined as the summing up all the possible paths between the source and destination. If any of the path has lesser weight, that path will be assigned as shortest path.

The distance (D) between the source node and destination node is defined as,

$$D(Ns, Nd) = D(Ns, Nc) + W(Nc, Nd) \tag{2}$$

where Nc is the cooperative node between the source and destination. C is the subset of the destination node and it belongs to the source node. From this we can rewrite the above equation as,

$$\begin{aligned} D(Ns, C) &= \min_{\substack{Ns \in S \\ Nd \in S}} D(Ns, C) + W(C, Nd) \\ &= \min_{Nd \in S} W(Ns, Nd) \end{aligned} \tag{3}$$

Based on the above calculation, we can determine weight of the link between the source and destination. By using the weight, source node will determine the shortest path to the destination node. LSAM is devised to mitigate the cooperative black hole attack and the analysis procedure is described. Once the Data Packet (DP) is transmitted to N_D from N_S, N_D acknowledges the data packet and sends acknowledgement (ACK) to N_S within a specific time interval $\Delta T1$.The number of data packets N_{DP} transmitted between Intermediate Hops (IH) is monitored for certain time interval $\Delta T2$. If packets are dropped (P_{Drop}) continuously above the threshold value by the same node, then the sequence number (α) of that particular node is extracted. If it is found abnormal (α'(when compared to remaining nodes in the transmission range, Security Monitoring Node (SMN) initiates

the detection process of existence of any black hole nodes in the route. Packet may also get dropped due to link failure, congestion or due to some malicious activities while forwarding it. Algorithm 1 describes the flow of data communication between N_S and N_D.

Algorithm 1: Task of Source and Destination Node

```
If N_S transmits DP
        Wait for ΔT1
        If ACK is received within ΔT1
                Allow successive transmission of DP
        Else
                Checks for number of IH
                SMN compares N_DP between neighbor hops
                If P_Drop<Threshold
                Allow successive transmission of DP
                Else
                        Start cooperative black hole detection process
Endif
```

MAC layer of AODV protocol is modified to find the number of packets transmitted between the source and destination node. Packet monitoring is activated for specified time interval to detect the packet dropping with the maintained packet cache. In case, if the packet monitoring threshold is fixed with larger value then the overhead for detecting the malicious node would be more. Packet cache is periodically refreshed to keep the updated information about the sent and received packets by a particular node. Neighbor cache is also maintained to keep the list of fresh neighboring nodes. It accepts the limited number of neighboring nodes in its own proximity area.

Black hole node detection process is triggered, if the sequence number is found abnormal. Neighbor cache maintains the node identity and the respective sequence number. Comparison of sequence number takes place between a particular node and all other nodes in the same transmission range. If the sequence number is extremely distinguished as α' from other sequence numbers (α_1, α_2, α_3,…, α_n) in the neighbor cache list, then the node(s) will be suspected as malicious and those nodes will be pushed into the black list. The remaining SMNs are informed using ALARM packet to isolate the malicious node(s) entries from their routing table. The suspected nodes will not be considered to include in the route and alternate trusted route is selected for further communication. Algorithm 2 summarizes the activity performed by SMN to detect the malicious node.

Algorithm 2: Task of Security Monitoring Node

```
Extract α^(i to n) in the transmission path
Check α of the suspected node
If α is in consecutive order (α1,α2,α3,…..αn)
        Allow successive transmission of DP
ElseIf
        α is abnormal(α′)
        Move to suspected black list
        Inform remaining nodes
Endif
```

4 Simulation Analysis

The simulation experiment is carried out with network simulator 2.34 in LINUX Fedora 14. The proposed system is executed on a laptop with CORE^{TM}i3 CPU and 3 GB RAM. The various simulation parameters are used in this work are listed in Table 1. In NS2.34, the default configuration settings of a network area are considered as 1000 × 1000 m with 100, 200, 300, 400, 500 normal nodes. Both the physical and MAC 802.11 layers are included in the wireless extension of NS2. All normal nodes are moved in a Random-Way Point model (RWP) with random speed between 0 and 5 m/s. Each node in RWP moves to a certain position in network called waypoint, pauses for some time at that position and then repeats the same pattern of pause and movement. In addition, a pause time is limited to 10 s where the pause time refers to frequency of dynamic topological configuration. Source–destination pairs were randomly chosen for data communication, each send a User Datagram Protocol–Constant Bit Rate (UDP–CBR) data packet with a packet size of 512 B per second. While executing LSAM routing protocol the nodes are randomly located, black hole nodes are cooperatively leading to the black hole attack, along with several SMNs.

In order to measure the performance of the proposed system, six following metrics are chosen to study the network performance.

4.1 Packet Delivery Ratio

PDR is the ratio of number of packets received by the destination node to the total number of packets transmitted by the source node. PDR is calculated as follows,

$$PDR = \frac{1}{k}\sum_{i=1}^{k}\frac{ndp_D}{ndp_S} \tag{4}$$

Here the number of packets received by the destination is ndp_D and the number of packets sent by the source node is ndp_S in the kth traffic. Hence it is clearly stated in Fig. 2 that PDR of AODV is greatly affected by the malicious nodes whereas the PDR of proposed AODV is immune to it. The PDR of AODV under attack was approximately 57 % while the PDR of LSAM was approximately 83 %, increased by 27 %.

Table 1 Simulation parameters

Parameters	Value
Simulator	Ns-2(ver.2.34)
Simulation time	1000 s
Number of nodes	100, 200, 300, 400, 500
Routing protocol	AODV
Traffic model	CBR
Pause time	10 (s)
Maximum mobility	5 m/s
Load	5 KB UDP packets, Data Payload 512 bytes
Terrain area	1000 m × 1000 m
Transmission range	250 m
No. of malicious nodes	0–40 %

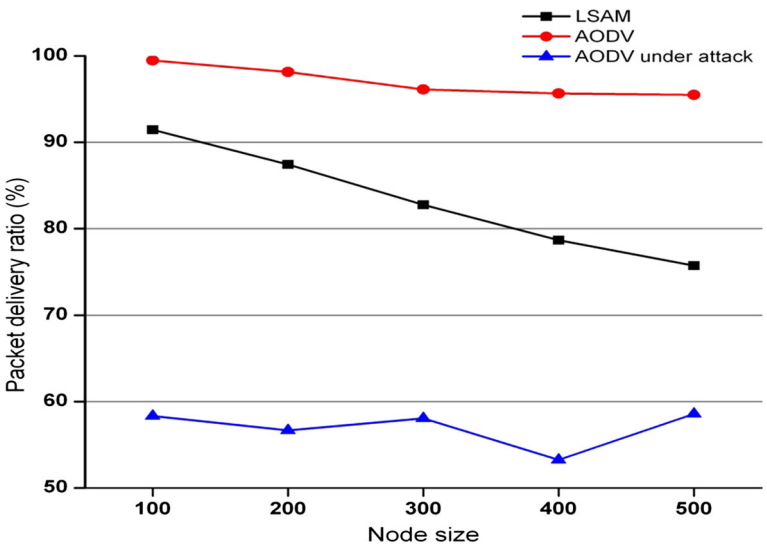

Fig. 2 Packet delivery ratio versus node size

4.2 Routing Overhead

It is the ratio of routing total number of control packets associated to data packets and it is also the number of routing packets sent per data packet delivered. RO can be calculated using the given formula,

$$RO = \frac{1}{k}\sum_{i=1}^{k}\frac{ncp}{ndp} \tag{5}$$

Here, *ncp* is the number of control packets and *ndp* is the number of data packets in the *k*th network traffic. It is shown in Fig. 3 that the routing overhead is more in the presence of black hole nodes. In LSAM, the effect of black hole nodes is greatly reduced and is slightly more when compared to normal AODV because due of the activities performed by SMNs. Routing overhead of AODV under attack is about 8 % but in LSAM is only 4 %.

4.3 End-to-End Delay

It is the average time taken for data packets successfully delivered to the destination. The total delay of packets received by the destination node is td_D and the number of packets received by the destination node is ndp_D in the *k*th network traffic. The formula for finding the delay is given below,

$$EED = \frac{1}{k}\sum_{i=1}^{k}\frac{td_D}{ndp_D} \tag{6}$$

End-to-end delay for delivering data packets to the destination is upgraded in this approach. Thus, the black hole detection process is initiated only after partially confirming the existence of malicious nodes. If there is no malicious node in the transmission path, then end-to-end delay is minimized as there is no overhead for detecting it. SMN traces the

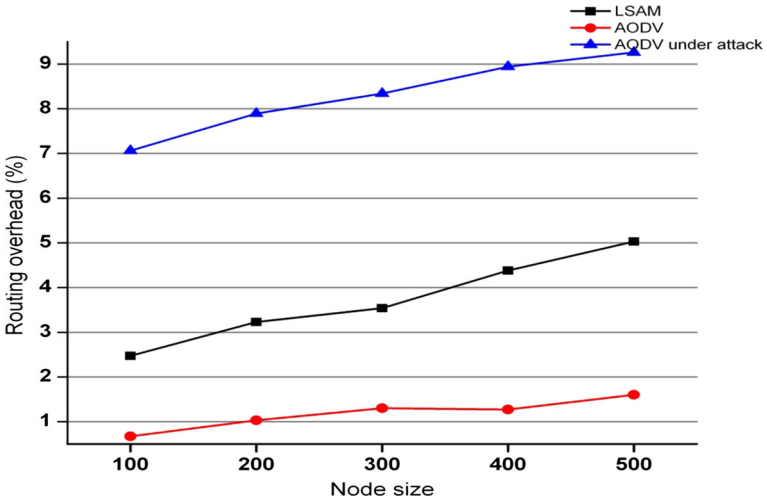

Fig. 3 Routing overhead versus node size

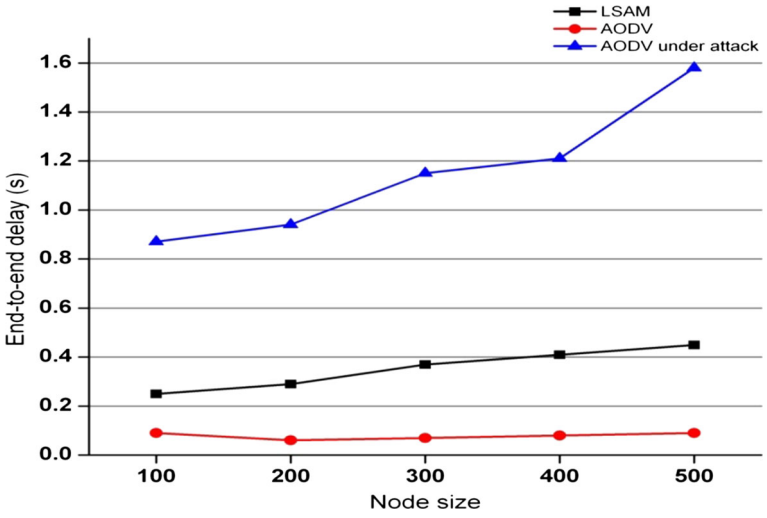

Fig. 4 End-to-end delay versus node size

suspected nodes and then it will be pushed to the black list. EED of AODV under attack is 0.9 % while EED of LSAM is about 0.3 % and the performance is shown in Fig. 4.

4.4 Throughput

Throughput is defined as the ratio of number of packets successfully received with respect to the simulation time. Figure 5 shows the throughput analysis by varying the number of nodes from 100 to 600. The bandwidth channel is assigned in between the source node and destination node which is approximately 2 Mbps.

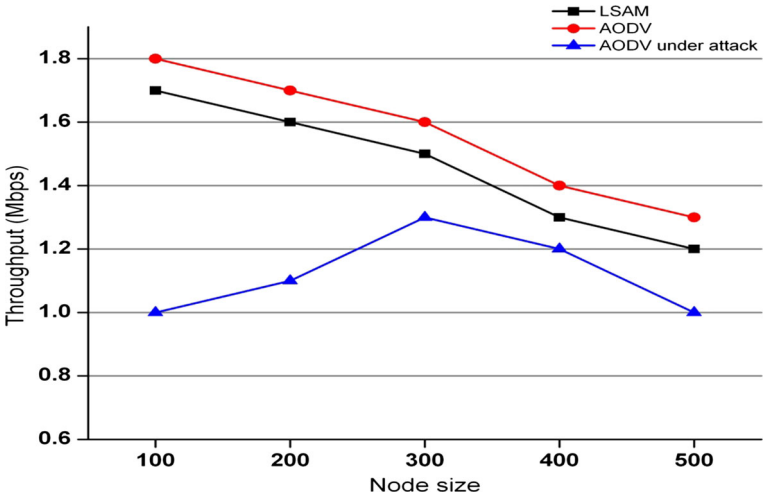

Fig. 5 Throughput versus node size

The AODV under attack has achieved lesser throughput of 1 Mbps from the bandwidth of 2 Mbps. The normal AODV routing protocol achieves more than the AODV under attack scheme. The proposed LSAM scheme has achieved 1.7 Mbps of throughput from the available bandwidth.

4.5 Packet Drop Rate

Packet drop rate is defined as the ratio of difference between the number of packets transmitted and the number of packets received with respect to the number of packets received.

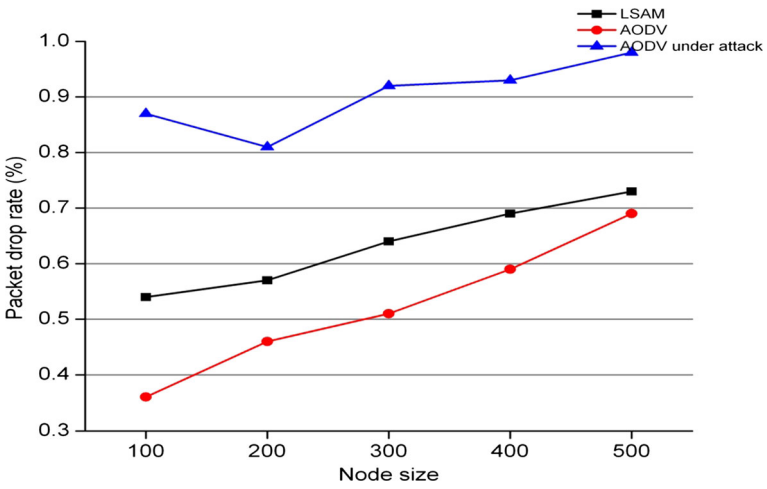

Fig. 6 Packet drop rate versus node size

$$PDr = \frac{1}{k}\sum_{i=1}^{k}\frac{ndp_S - ndp_D}{ndp_D} \tag{7}$$

where ndp_S is the number of packets sent by the source and ndp_D is the number of packets successfully received by the destination in the kth traffic. Figure 6 shows that the PDr by varying the number of nodes from 100 to 500. Here drop rate has decreased in the proposed LSAM routing scheme. Due to the black hole attacks, AODV under attack has high drop rate of 90 % and the proposed LSAM scheme has lesser drop rate of 63 %.

4.6 Control Overhead

Control overhead is defined as the number of control messages received with respect to the simulation time. To detect the black hole attack, it requires more number of control messages and this control overhead can increase the traffic rate and reduce the network performance. Figure 7 shows the control overhead versus number of nodes varying from 100 to 600 nodes. By decreasing the control overhead, the network performance can be increased. The AODV under attack has increased the control overhead due to the black

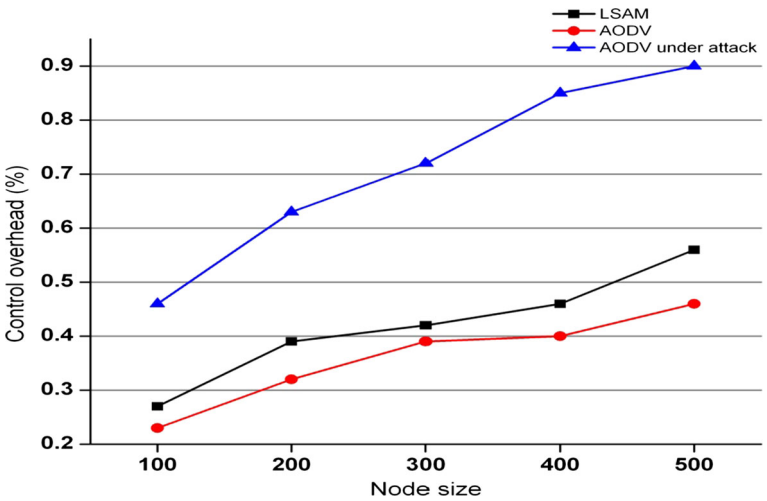

Fig. 7 Control overhead versus node size

Table 2 Comparison of QoS parameters

Parameters	AODV under attack	Normal AODV	LSAM
Number of nodes	500	500	500
Packet delivery ratio (%)	57	97	83
Routing overhead (%)	8	1	4
Throughput (Mbps)	1.2	1.9	1.7
End to end delay (S)	0.96	0.07	0.35
Packet drop rate (%)	90	52	63
Control overhead (%)	71	36	42

hole attack. The proposed LSAM has less control overhead in the presence of 40 % of malicious nodes. This scheme uses the lesser number of control messages to detect the black hole attacks.

Table 2 shows that the comparison of quality of service parameters such as PDR, RO, Th, EED, PDr and CO. The proposed LSAM has high delivery rate and throughput and it decreases the EED, RO, CO and drop rate in the presence of 40 % of misbehaving nodes in the mobile ad hoc network.

5 Conclusion

In this proposed methodology, a novel LSAM protocol is specially designed for providing security in MANET and it is compared with normal AODV protocol in various scenarios through simulation. The simplest technique is designed to detect and prevent malicious activities against co-operative black hole attack. Even though it generates little overhead as shown in the experiment, it greatly improves the network's PDR when the attackers are trying to forge or drop the packets. The simulation result shows that the LSAM outperforms in terms of PDR, routing overhead and end-to-end delay, packet drop rate, throughput and control overhead. PDR is increased by 27 % in the presence of 40 % misbehaving nodes, while it increases the percentage of overhead of proposed routing protocol from 1 to 4 %. EED is greatly reduced from 0.9 to 0.3 % in LSAM.

References

1. Zhou, L., & Haas, Z. (1999). Securing ad hoc networks. *IEEE Network Magazine*, *13*, 24–30.
2. Zapata, M., & Asokan, N. (2002). Securing ad hoc routing protocols. In *Proceedings of 3rd ACM workshop WiSE*, pp. 1–10.
3. Papadimitratos, P., & Haas, H. (2003). Secure data transmission in mobile ad hoc networks. In *Proceedings of ACM workshop WiSE*, pp. 41–50.
4. Yih-Chun, H, & Perrig, A. (2004). A survey of secure wireless ad hoc routing. *IEEE Security Privacy*, *2*, 28–39.
5. Sanzgiri, K., Dahill, B., Levine, B. N., Shields, C., & Belding-Royer, E. M. (2002). A secure routing protocol for ad hoc network. In *Proceedings of 10th IEEE International Conference in Network Protocols (INCP' 02)*, IEEE press (pp. 78–87).
6. Deng, H., & Agarwal, P. (2002). Routing security in wireless ad hoc networks. *IEEE Communication Magazine, 40*, 70–75.
7. Perkins, C., Belding-Royer, E., & Das, S. (2003). Ad hoc on-demand distance vector (AODV) routing. IETF RFC, 3561.
8. Marti, S., Giuli, T. J., Lai, K., & Baker, M. (2000). Mitigating routing misbehaviour in mobile ad hoc networks. In *Proceedings of the 6th annual international conference mobile computer networks*, pp. 255–265.
9. Wang, B., Chen, X., & Chang, W. (2014). A light-weight trust-based QoS routing algorithm for ad hoc networks. *Pervasive and Mobile Computing, 13*, 164–180.
10. 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*, 1162–1174.
11. Sánchez-Casado, L., Maciá-Fernández, G., García-Teodoro, P., & Magán-Carrión, R. (2015). A model of data forwarding in MANETs for lightweight detection of malicious packet dropping. *Computer Networks, 87*, 44–58.
12. Nadeem, A., & Howarth, M. P. (2014). An intrusion detection & adaptive response mechanism for MANETs. *Ad Hoc Networks, 13*, 368–380.
13. Nakayama, H., Kurosama, S., Jamalipour, A., Nemoto, Y., & Kato, N. (2009). A dynamic anomaly detection scheme for AODV-based mobile ad hoc networks. *IEEE Transactions on Vehicular Technology, 58*, 2471–2481.

14. Ming-Yang, S. (2011). Prevention of selective black hole attacks on mobile ad hoc networks through intrusion detection systems. *Computer Communication, 34*, 107–117.
15. Kurosawa, S., Nakayama, H., Kato, N., Jamalipour, A., & Nemoto, Y. (2007). Detecting blackhole attack on AODV-based mobile ad hoc networks by dynamic learning method. *International Journal of Network Security, 5*, 338–346.
16. Latha, T., & Sankaranarayanan, V. (2008). Prevention of co-operative black hole attack in MANET. *Journal of Networks, 3*, 13–20.
17. Shakshuki, E. M., Kang, N., & Sheltami, T. (2013). EAACK—A secure intrusion-detection system for MANETs. *IEEE Transactions on Industrial Electronics, 60*, 1089–1098.
18. Network Simulator-NS (ver. 2). http://nsnam.isi.edu/nsnam/

T. Poongodi received M.Tech., in Information Technology from Anna University in 2009. She is currently working as an assistant professor in PPG Institute of Technology, Coimbatore, India. She has 10 years of teaching experience in the field of computer science. Her recent research work is focused on ad hoc routing protocols and network security. Her area of interest lies in the field of wireless networking, particularly ad hoc network security, data mining, theory of computation, compiler design, software engineering.

Dr. M. Karthikeyan received B.E. degree in Electronics and Communication Engineering from Bharathiar University, Coimbatore, India in 1990. Subsequently received his M.Tech., and Ph.D., degrees in Computer and Information Technology from Centre for Information Technology and Engineering, Manonmaniam Sundaranar University, Tirunelveli, India. His research interests include data mining, wireless communication and image Processing. He is a senior Member of the IEEE, secretary of IEEE podhigai sub-section of Madras section and life member of ISTE. He is currently working as the Principal, Tamilnadu College of Engineering, Coimbatore, India.