Wireless Networks
https://doi.org/10.1007/s11276-017-1640-9

A time stamp-based algorithm to improve security and performance of mobile ad hoc network

S. D. Ubarhande[1] · D. D. Doye[1] · P. S. Nalwade[1]

Abstract
Mobile ad hoc network is open medium and infrastructure-less network. Mobile ad hoc network is susceptible to various security attacks such as, black hole attack, gray hole attack, bad mouthing attack, sybil attack and worm hole attack due to open medium, infrastructure-less features and lack of in-built security. In black hole attack and gray hole attack, attacker falsely sends route reply and dropped data packets received from source node. Due to these attacks, performance of mobile ad hoc network decreases. This paper proposes a time stamp-based algorithm which is an enhanced version of existing IDSNAODV algorithm. Proposed algorithm modifies existing palling process to validate identity of observer nodes using a time stamp-based approach. Based on defined set of rules and recorded activities report, source node decides the nature of target node. The performance of proposed algorithm is evaluated using the network simulator. The proposed algorithm shows improved performance for packet delivery ratio, throughput and routing overhead as compared to existing algorithm.

Keywords Mobile ad hoc network · Security attacks · IDSNAODV algorithm · Time stamp-based algorithm

1 Introduction

1.1 Mobile ad hoc network

Mobile ad hoc network (MANET) is self-configuring [1, 2] and decentralized network [3–5] in which each node behave as a host as well as a router [6, 7]. Dynamic topology of MANET offers unlimited mobility to nodes [8]. Due to open medium and lack of inbuilt security mechanism, MANET is vulnerable to various security attacks. Attacks in MANET are classified as passive attacks and active attacks [9]. In passive attack such as eavesdropping attack, an attacker node without disturbing normal working of network passively monitors the network traffic. In an active attack, an attacker node disturb the normal working of network. The examples of an active attacks are black hole attack [10–13], gray hole attack [14, 15], bad mouthing attack [8], sybil attack [16] and worm hole attack [17]. In black hole attack, attacker node falsely sends route reply to source node. Source node then sends data packets to attacker. Attacker node drops all data packets received from source node [4]. In gray hole attack, attacker node sends false route reply to source node and then selectively drop data packets received from source node. In bad mouthing attack, bad nodes provide negative rating about good nodes in network. Negative rated nodes are not allowed to participate in any network activity. In Sybil attack, attacker node generates its own multiple false identities. In worm hole attack, attacker nodes build a tunnel and diverts entire traffic to desire destination.

The security solutions for MANET are classified into two main types: prevention and detection [18]. Prevention technique such as encryption is expensive [18] due to limited resources of MANET. As regard the latter, intrusion detection system [18–20] is required, in order to detect and isolate attackers from active path. This paper proposes the enhanced version of IDSNAODV algorithm namely a time stamp-based (TSB) algorithm. Proposed TSB algorithm modifies the existing palling process of IDSNAODV algorithm to validate

✉ S. D. Ubarhande
sachin1356@gmail.com

D. D. Doye
dddoye@yahoo.com

P. S. Nalwade
psnalwade@yahoo.com

[1] Shri Guru Gobind Singhji Institute of Engineering and Technology, Nanded, India

Published online: 12 December 2017

identity of observer nodes by using a time stamp-based value. The observer nodes involved in palling process record activities of target node. The observer nodes then sends activities report to source node. The source node then decides the nature of target node. The draw back of IDSNAODV algorithm is false misbehavior report due to involvement of attacker nodes in palling process. As there is no scheme to validate authenticity of nodes involved in palling process, it increases false positive probability and decreases throughput and packet delivery ratio. The proposed TSB algorithm provides validation scheme for nodes involving in palling process. In which, observer nodes need to send a time stamp-based value to source node. If time stamp value is matched at source node, then the report is accepted at source node. The advantages of proposed system as compared to existing system are:

1. Proposed TSB system reduces false positive probability (i.e. less failure rate of system to treat good node as attacker as compared to existing IDSNAODV [4] system).
2. Existing system can handle only black hole attack, whereas proposed algorithm handles both black hole attack and gray hole attack.
3. Proposed TSB system does not add extra overhead in network.

The only disadvantage of proposed system is that, it can handle only black hole attack and gray hole attack. The paper is organized as: Sect. 1 presented introduction, Sect. 2 discusses re-lated work and Sect. 3 explains the proposed algorithm. Section 4 discusses the simulation environment and results. Section 5 concludes the paper.

2 Related work

Raza and Hussain [21] have proposed guard nodes based attacker detection mechanism. In guard node detection mechanism, initially all nodes are assigned a minimum trust level. Based on the observed behavior, guard nodes change trust level of target node. If trust level goes below threshold trust level, then target node is treated as attacker.

Sanchez-Casado et al. [22] have proposed a lightweight window analysis system to detect attackers in MANET. The window analysis technique collects the network features of nodes. The collected features are then used to decide the behavior of node.

Nadeem and Howarth [23] have proposed a intrusion detection system for mobile ad hoc network. The system performs the audit on network data to distinguish between normal traffic and malicious traffic. The audit data is then used to train the system to detect attackers.

Das et al. [24] have proposed a game theory approach to detect selfish nodes in MANET. The game theory approach works based on set of defined rules. Defined rules for selfish node are: node which does not forward Route Request (RREQ) packet, will not forward the data and delays forwarded RREQ packet.

Kumar et al. [9] have proposed a token based umpire technique to detect selfish node in MANET. Selfish node is a node which utilizes network resources and refuses to help other nodes. In umpire technique, all nodes in the network shares routing table with each other. The routing table consist of three fields namely, status flag as green, ID and zero as reputation value. If any node changes default value during path setup then node is treated as selfish.

Khatawkar and Trivedi [14] have proposed a cluster analysis technique to detect attacker in network. In cluster analysis technique, home agent is generated. The home agent is then migrated to target node. If observer node receives reply from target node then target node is treated as good node otherwise as a malicious.

Shakshuki et al. [25] have proposed a EAACK intrusion detection system for MANET. EAACK system consist of ACK scheme, secure ACK scheme and MRA scheme. ACK is an end to end acknowledgment scheme, which helps to reduce routing overhead in absence of attacker. If malicious behavior is detected the system is switched to SACK scheme. SACK scheme detects attacker in a group of three consecutive nodes. Finally, system switches to MRA scheme to validate SACK report.

Shahabi et al. [4] have proposed IDSNAODV algorithm for MANET to protect from black hole attack. IDSNAODV algorithm uses the palling process to record activities of target node. The observer nodes then send activities report to source node. Based on received activities report and set of defined rules, source node decides the behavior of target node. If attacker is detected, the alert is broadcast in network to quarantine attacker node. The weaknesses of IDSNAODV algorithm are lacking of observer nodes validation involved in palling process. IDSNAODV algorithm cannot handle false misbehavior report received from attacker nodes.

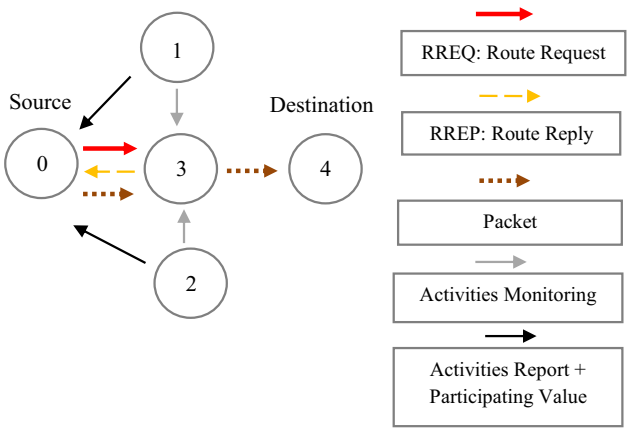

Fig. 1 Architecture of proposed TSB system

IDSNAODV algorithm also suffers from high false positive probability which degrades the performance of network. Existing system can only able to handle only black hole attack.

3 The proposed system

Figure 1 shows the architecture of proposed system. The proposed system overcomes the weaknesses of IDS-NAODV system. Proposed system validates observer nodes by introducing a time stamp-based approach, in which, observer node sends a generated time stamp-based value to source node. The activities report from observer node is accepted only when its time stamp-based value is matched at source node. Based on defined rules, source node then decides the nature of target node. Source node 0 broadcast RREQ packet in network to establish a path with a destination node 4. After receiving RREQ from node 0, node 3 replies by sending Route Reply (RREP) packet. Source node then sends data packet to node 3. During packet transmission from node 0 to node 4 via node 3, observer node 1 and node 2 records activities of new node 3 involving in current active path. Node 1 and node 2 then sends activities report and generated participating value to source node 0. For simulation purpose, participating value is taken as 1. To ensure maximum security, one should take more number of participating values which is based on present time stamp. If participating value of observer node is matched at source node then source node accepts activities report. Otherwise source node discards activities report. Based on received activities report and defined set of rules, source node decide the behavior of target node. If malicious behavior is detected, then source node broadcast the alert in network to quarantine malicious node.

3.1 Proposed TSB algorithm

Figure 2 shows the flowchart of the proposed TSB system. Based on following assumptions, the proposed TSB system works:

Algorithm 1: Proposed TSB algorithm

Start:
Source broadcast RREQ
if *RREP receives: yes* **then**
  go to next step
else
  go to Start
end
if *RREP from quarntine node: yes* **then**
  Discards RREP
else
  go to next step
end
if *RREP from new node: no* **then**
  Source sends data packets and go to step 25
else
  go to next step
end
Source sends data packets
Observer nodes record activities of responder node
Observer nodes sends activities report and time stamp-based participating value to source node
if *Participating value matched: yes* **then**
  Source accepts activities report
else
  Source discards activities report
end
Source decides nature of responder node and if requires broadcast the alert in network
End

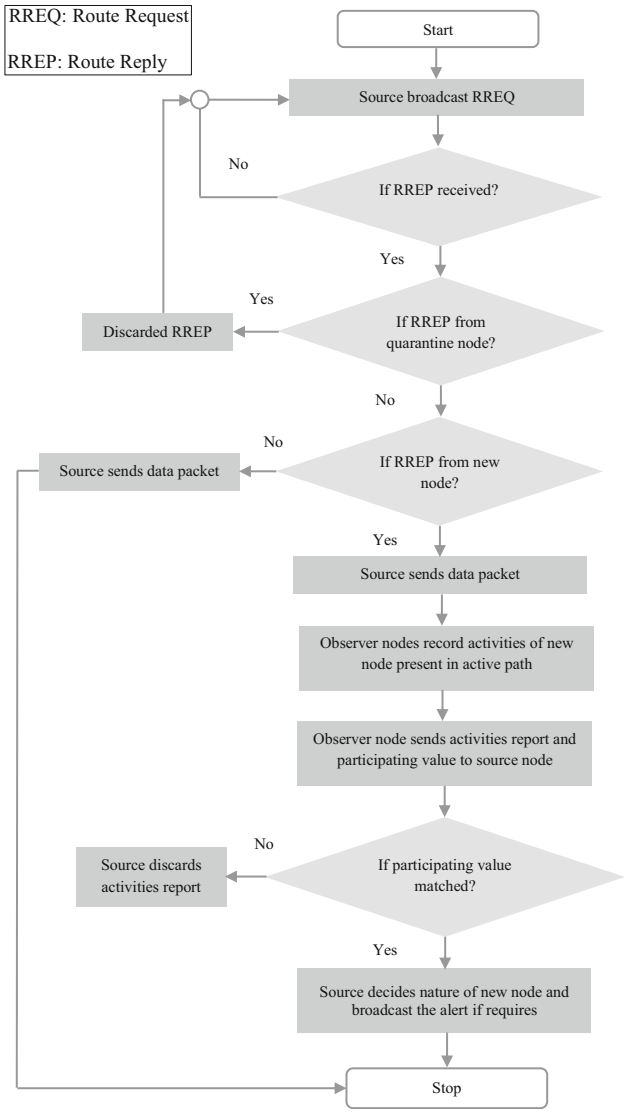

Fig. 2 Flow chart of the proposed TSB system

1. Initially, only legitimate nodes are present in network which share time stamp-based participating values.
2. Nodes nature is static and does not convert from legitimate to malicious and vice-versa.
3. All nodes in network maintain both attacker list and trusted node list.
4. To generate exact time stamp-based participating value, all nodes are assumed to have synchronized clock time
5. For simulation purpose, valid participating value is taken as 1.
6. The neighbor of target nodes acts as observer nodes.

In TSB algorithm, source node broadcast RREQ packet in network to establish a path to destination node. The neighbor nodes after receiving RREQ packet further broadcasts to their neighbor nodes. If any node receives RREP packet from responder node, then entry of responder node is checked in quarantine list. If responder node is located in quarantine list then RREP packet from responder node is discarded. Otherwise source node sends data packet to destination node via established path. If responder node is new then observer nodes record new node activities. Observer node sends activities report plus generated participating value to source node. If participating value sent by observer node is matched at source node, then source node accepts the activities report. Otherwise source node discards received activities report. Base on received activities report and set of defined rules, source node decides the nature of new node. The set of defined rules are:

1. In black hole attack, the node which receives a great number of packets and does not forward any packet is the attacker node.
2. In gray hole attack, the node which receives a great number of packets and forwards only few packets, (i.e. packet delivery ratio is $< 90\%$) then node is attacker.

4 Simulation

4.1 Simulation environment

The results of TSB algorithm are compared with IDS-NAODV algorithm [4] using the Network Simulator (NS2). NS2 is a discrete event simulator targeted at networking research. NS2 provides substantial supports for simulation of routing protocols over wireless networks. The propagation model used is a two ray ground. The two ray ground reflection model considers both the direct path and a ground reflection path. The antenna used is an omni directional antenna which radiates radio wave power uniformly in all directions in one plane. The MAC type is 802.11. The 50 nodes are deployed in 1000 m $\times$ 1000 m environment size. The first scenario is run for 900 s for varying number of attackers from 2 to 20 under black hole attack and the second scenario is run under 900 s for varying number of attackers from 2 to 20 under gray hole attack. The simulation parameters are shows in Table 1.

4.2 Performance metrics

1. *Packet delivery ratio* Packet delivery ratio [4] is the ratio of total data packets received at the destination to the total data packets transmitted by the source. With increase in number of attackers, packet delivery ratio decreases.
2. *Routing overhead* Is the ratio of total routing related packets generated to the total packets generated during

entire transmission. With increase in number of attackers, number of routing packets increases in network. As a result, the system without attacker detection mechanism will generate more routing overhead in network.

3. *Packet loss rate* Packet loss rate [4] is number of total data packets lost during entire transmission. With increase in number of attackers, packet loss rate increases as more attackers join active path.
4. *Throughput* Throughput [4] is the total number of data packets successfully received by destination during entire transmission. If number of attackers are more in network then destination node receives less data packets, as attackers present in active path do not forward data packets towards destination node.

4.3 Simulation results

In first scenario, performance of the TSB algorithm is compared with IDSNAODV algorithm under black hole attack for varying number of attackers.

In black hole attack, false positive probability that is percentage of system to detect good node as malicious node is 0.99% in TSB algorithm, while for IDSNAODV algorithm it is 1.96% due following reasons:

1. False positive probability in IDSNAODV algorithm is considered due to non-validation of nodes involved in activities monitoring.
2. False positive probability is considered for both the algorithms if in-case no observer node is available for activities monitoring.

Table 1 Simulation parameters

Parameter	Value
Simulator	NS2
Simulation time	900 s
Number of nodes	50
Malicious nodes	2–20
Channel type	Wireless channel
Antenna	Omni directional
Environment size	1000 m × 1000 m
Mobility model	Random way point
Routing protocol	IDSNAODV and TSB
MAC protocol	802.11
Traffic type	CBR
Propagation model	Two ray ground
Packet size	512 byte

Mathematically false positive probability of both systems under black hole attack:

$$\text{TSB False Positive Probability} = \frac{P(G/A) * P(G)}{P(T)} = \frac{1\% * 99\%}{100\%} = 0.99\%$$

$$\text{IDSNAODV False Positive Probability} = \frac{P(G/A) * P(G)}{P(T)} = \frac{2\% * 98\%}{100\%} = 1.96\%$$

Where,

P(G/A) is the probability to detect good node as attacker
P(G) is the probability to detect good nodes
P(T) is the probability of total number of nodes

Obtained results are average of ten runs. Figure 3(a) packet delivery ratio of TSB and IDSNAODV algorithms verses number of attackers. It is observed that in an average TSB delivered 89.11% while IDSNAODV delivered 75.84% packet delivery ratio. It is also observed that TSB algorithm shows moderate packet delivery ratio even number of attacker are increased from 2 to 20.

Figure 3(b) compares throughput of TSB algorithm with IDSNAODV algorithm. It is observed that TSB algorithm delivered good throughput for increased number of attackers. In an average, TSB delivered 458 bps throughput, while IDSNAODV delivered 167 bps throughput. More throughput in TSB is due to less number of packets dropped.

Figure 3(c) compares routing overhead of TSB algorithm against IDSNAODV algorithm. From figure, it is observed that with increase in number of attackers from 2 to 20, TSB algorithm delivered less routing overhead as compared IDSNAODV algorithm.

Figure 3(d) compares number of packet loss against varying number of attackers. It is observed that throughout the simulation time, TSB algorithm exhibited moderate number of packet loss rate. It is also observed that number of packet loss is slightly more in TSB algorithm than IDSNAODV algorithm. As in TSB algorithm, source nodes send more number of data packets, so more number of packet loss which is also due to frequent link breakages.

In second scenario performance of TSB algorithm is compared against ID-SNAODV algorithm under gray hole attack for varying number of attackers. In gray hole attack false positive probability that is percentage of system to detect good node as malicious node is 0.99% in TSB algorithm, while in IDSNAODV algorithm false positive probability is considered as 2.91% due following reasons:

1. False positive probability in IDSNAODV algorithm is considered due to non-validation of nodes involving in palling process.

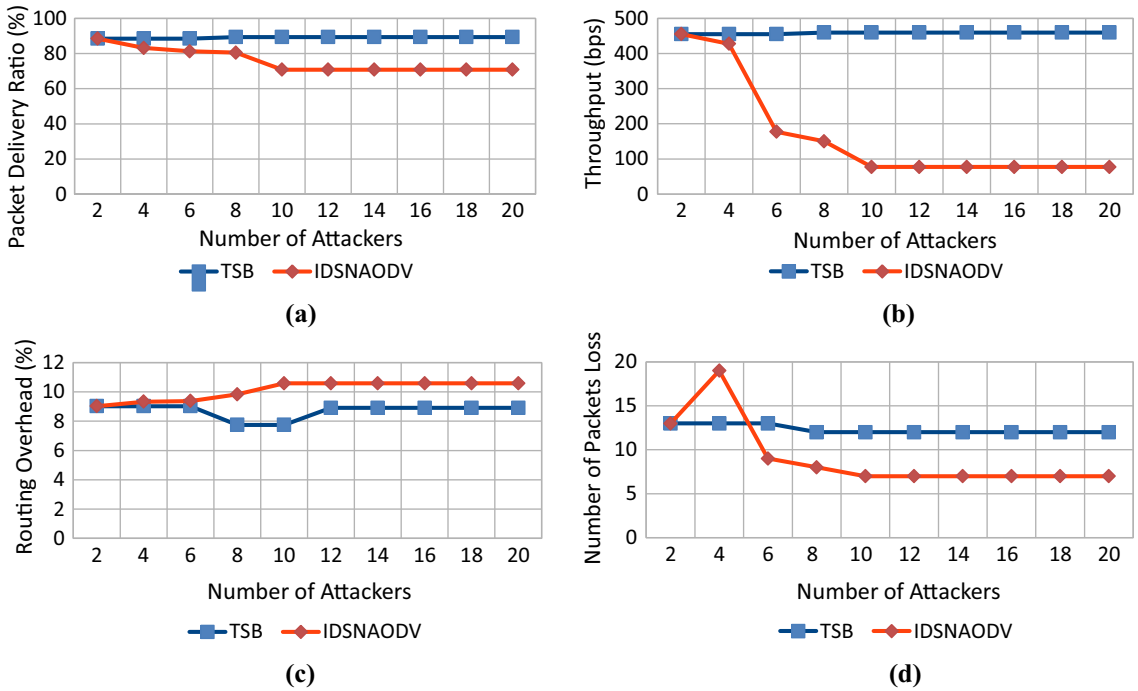

Fig. 3 **a** Packet delivery ratio, **b** throughput, **c** routing overhead and **d** packet loss rate verses number of attackers under black hole attack

2. False positive probability is considered for both the algorithms if in-case no observer node is available for activities monitoring.
3. False positive probability in IDSNAODV algorithm is considered due to absence of threshold limit for packet delivery ratio, whereas in TSB algorithm packet delivery ratio threshold value is set as 90%.

Mathematically false positive probability of both systems under gray hole attack:

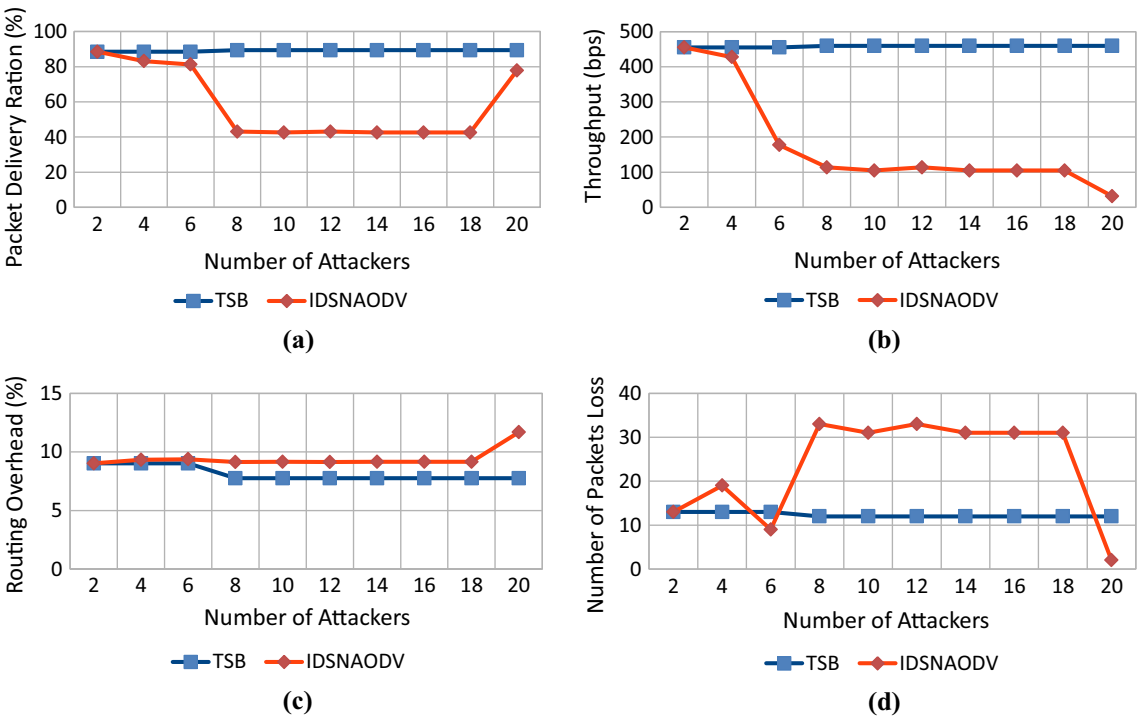

Fig. 4 **a** Packet delivery ratio, **b** throughput, **c** routing overhead, **d** packet loss rate verses number of attackers under gray hole attack

TSB False Positive Probability

$$= \frac{P(G/A) * P(G)}{P(T)} = \frac{1\% * 99\%}{100\%} = 0.99\%$$

IDSNAODV False Positive Probability

$$= \frac{P(G/A) * P(G)}{P(T)} = \frac{3\% * 97\%}{100\%} = 2.91\%$$

Where,

P(G/A) is the probability to detect good node as attacker
P(G) is the probability to detect good nodes
P(T) is the probability of total number of nodes

Figure 4(a) shows comparison of packet delivery ratio verses number of attackers. From Fig. 4(a) it is observed that proposed TSB algorithm delivered high packet delivery ratio as compared to IDSNAODV algorithm when attackers increased from 2 to 20. While TSB algorithm delivered moderate packet delivery ratio.

Figure 4(b) compared throughput of TSB algorithm with IDSNADOV algorithm. It is observed that TSB algorithm delivered high throughput even if number of attacker are increased from 2 to 20. The high throughput is result of accurate attacker detection process of proposed TSB algorithm.

Figure 4(c) compares routing overhead of TSB and IDSNAODV algorithms. In an average, TSB algorithm delivered 8.1% routing overhead, while IDSNAODV algorithm delivered 9.4% routing overhead.

Figure 4(d) compared number of packet loss of both the algorithms. From Fig. 4(d) it is observed that in an average, TSB delivered 12 number of packet loss for simulation time of 900 s. While IDSNAODV algorithm, delivered 23 number of packets loss in an average, for 900 s simulation time.

5 Conclusions and future work

This paper presented a time stamp-based algorithm to improve security and performance of MANET under black hole attack and gray hole attack. The performance of proposed TSB algorithm is compared against IDSNAODV algorithm using NS2 network simulator for varying number of attackers. The obtained results show that the TSB algorithm delivered high packet delivery ratio, high throughput and less routing overhead as compared to IDSNAODV algorithm. In future work, we shall modify the proposed algorithm to handle other types security attacks in MANET, such as sybil attack and worm hole attack.

References

1. Alkhamisi, A. O., & Buhari, S. M. (2016). Trusted secure adhoc on-demand multipath distance vector routing in MANET. In *30th International conference on advanced information networking and applications (AINA)* (pp 212–219). IEEE.
2. Moudni, H., Er-rouidi, M., Mouncif, H., & El Hadadi, B. (2016). Modified AODV routing protocol to improve security and performance against black hole attack. In *International conference on information technology for organizations development (IT4OD)* (pp. 1–7). IEEE.
3. Chang, J. M., Tsou, P. C., Woungang, I., Chao, H. C., & Lai, C. F. (2015). Defending against collaborative attacks by malicious nodes in MANETs: A cooperative bait detection approach. *IEEE Systems Journal*, *9*(1), 65–75.
4. Shahabi, S., Ghazvini, M., & Bakhtiarian, M. (2015). A modified algorithm to improve security and performance of AODV protocol against black hole attack. *Wireless Networks*, *22*(5), 1505–1511.
5. Mylsamy, R., & Sankaranarayanan, S. (2016). A preference-based protocol for trust and head selection for cluster-based MANET. *Wireless Personal Communications*, *86*(3), 1611–1627.
6. Babu, M. R., Dian, S. M., Chelladurai, S., & Palaniappan, M. (2015). Proactive alleviation procedure to handle black hole attack and its version. *The Scientific World Journal*, *2015*, 715820. https://doi.org/10.1155/2015/715820.
7. Raja, K., Deivasigamani, A., & Ravi, V. (2015). A reliant certificate revocation of malicious nodes in MANETs. *Wireless Personal Communications*, *90*(2), 435–455.
8. Shabut, A. M., Dahal, K. P., Bista, S. K., & Awan, I. U. (2015). Recommendation based trust model with an effective defence scheme for MANETs. *IEEE Transactions on Mobile Computing*, *14*(10), 2101–2115.
9. Kumar, J. M. S. P. J., Kathirvel, A., Kirubakaran, N., Sivaraman, P., & Subramaniam, M. (2015). A unified approach for detecting and eliminating selfish nodes in MANETs using TBUT. *EURASIP Journal on Wireless Communications and Networking*, *2015*(1), 1–11.
10. Jain, A. K., & Tokekar, V. (2015). Mitigating the effects of Black hole attacks on AODV routing protocol in Mobile Ad hoc Networks. In *International conference on pervasive computing (ICPC)* (pp. 1–6). IEEE.
11. Arthur, M. P., & Kannan, K. (2016). Cross-layer based multiclass intrusion detection system for secure multicast communication of MANET in military networks. *Wireless Networks*, *22*(3), 1035–1059.
12. Soleimani, M. T., & Kahvand, M. (2014). Defending packet dropping attacks based on dynamic trust model in wireless ad hoc networks. In *17th mediterranean electrotechnical conference* (pp. 362–366). IEEE.
13. Kavitha, P., & Mukesh, R. (2015). To detect malicious nodes in the mobile ad-hoc networks using soft computing technique. In *2nd International conference on electronics and communication systems (ICECS)* (pp. 1564–1573). IEEE.
14. Khatawkar, S. D., & Trivedi, N. (2015). Detection of gray hole in MANET through cluster analysis. In *2nd international conference on computing for sustainable global development (INDIACom)* (pp. 1752–1757). IEEE.
15. Jhaveri, R. H., & Patel, N. M. (2015). A sequence number based bait detection scheme to thwart grayhole attack in mobile ad hoc networks. *Wireless Networks*, *21*(8), 2781–2798.
16. Abbas, S., Merabti, M., Llewellyn-Jones, D., & Kifayat, K. (2013). Lightweight sybil attack detection in MANETs. *IEEE Systems Journal*, *7*(2), 236–248.

17. Raja, K., Deivasigamani, A., & Ravi, V. (2016). A reliant certificate revocation of malicious nodes in MANETs. *Wireless Personal Communications*, *90*(2), 435–455.
18. Hidoussi, F., Toral-Cruz, H., Boubiche, D. E., Lakhtaria, K., Mihovska, A., & Voznak, M. (2015). Centralized IDS based on misuse detection for cluster-based wireless sensors networks. *Wireless Personal Communications*, *85*(1), 207–224.
19. Nishani, L., & Biba, M. (2016). Machine learning for intrusion detection in MANET: A state-of-the-art survey. *Journal of Intelligent Information Systems*, *46*(2), 391–407.
20. Savner, J., & Gupta, V. (2014). Clustering of mobile ad hoc networks: An approach for black hole prevention. In *International conference on issues and challenges in intelligent computing techniques (ICICT)* (pp. 361–365). IEEE.
21. Raza, I., & Hussain, S. A. (2008). Identification of malicious nodes in an AODV pure ad hoc network through guard nodes. *Computer Communications*, *31*(9), 1796–1802.
22. Snchez-Casado, L., Maci-Fernndez, G., Garca-Teodoro, P., & Magn-Carrin, R. (2015). A model of data forwarding in MANETs for lightweight detection of malicious packet dropping. *Computer Networks*, *87*, 44–58.
23. Nadeem, A., & Howarth, M. P. (2014). An intrusion detection & adaptive response mechanism for MANETs. *Ad Hoc Networks*, *13*, 368–380.
24. Das, D., Majumder, K., & Dasgupta, A. (2015). Selfish node detection and low cost data transmission in MANET using game theory. *Procedia Computer Science*, *54*, 92–101.
25. Shakshuki, E. M., Kang, N., & Sheltami, T. R. (2013). EAACKa secure intrusion-detection system for MANETs. *IEEE Transactions on Industrial Electronics*, *60*(3), 1089–1098.

S. D. Ubarhande received his Bachelor's degree in Computer Science and Engineering and Master's degree in Software Systems. From September 2014, he is working as a full-time Ph.D. Research Scholar at Shri Guru Gobind Singhji Institute of Engineering and Technology, Nanded, India. His research interests are in the area of wireless communication, mobile ad hoc networks and security for wireless systems.

D. D. Doye received his Ph.D. in Electronics and Telecommunication Engineering from Shri Guru Gobind Singhji Institute of Engineering and Technology, Nanded, India. Currently, he is working as a Professor in the Electronics and Telecommunication Engineering Department at Shri Guru Gobind Singhji Institute of Engineering and Technology, Nanded, India. His key research interests include wireless networks, fuzzy neural networks, speech processing and image processing.

P. S. Nalwade received his Bachelor's degree in Computer Engineering and Master's degree in Electronics Engineering from Shri Guru Gobind Singhji Institute of Engineering and Technology, Nanded, India. Currently, he is working as an Associate Professor and Head of the Department of Computer Science and Engineering at Shri Guru Gobind Singhji Institute of Engineering and Technology, Nanded, India. His subjects of interest are computer networks, mobile and wireless networks, database systems and data mining.