Asian Journal of Information Technology 15 (23): 4890-4899, 2016
ISSN: 1682-3915

Mitigating Cooperative Black Hole Attack by Dynamic Defense Intrusion Detection Scheme in Mobile Ad Hoc Network

[1]T. Poongodi, [2]M. Karthikeyan and [1]D. Sumathi
[1]Department of Computer Science and Engineering, PPG Institute of Technology, Tamil Nadu, India
[2]Department of Electronics and Communication Engineering, College of Engineering, Tamil Nadu, India

Abstract: Major investigations have been focused on the security issues in Mobile Ad Hoc network (MANET) for the past few years. It requires continuous monitoring which lead to rapid exhaustion of node's battery life. Establishing communication among the self configuring nodes for transferring packets is a challenging task in MANET. In the presence of malicious nodes such task may be a great security concern; for instance, these nodes may interrupt the entire network process. To address these issues, threshold based light weight Energy Based Secure Routing (EBSR) protocol is proposed. The dynamic defense scheme is provided by comparing the context of interaction of nodes in the network. Each interaction describes the behavior within the operational scenario of the network. Set of interactions are determined analytically and the node's behavior are tracked dynamically during simulation. The simulation results show that the proposed technique significantly achieves better packet delivery ratio with less delay by detecting and isolating attacker nodes than existing techniques. It also reduces network traffic and the overall energy consumption by maintaining high detection rate and accuracy.

Key words: MANET, black hole attack, AODV routing, PDR, delay, false positive, false negative

INTRODUCTION

MANET consists of mobile nodes where each node acts as hosts as well as a router for forwarding packets. These networks are formed without any centralized coordinator or a base station. Due to its features like open medium, dynamic topological configuration it is more vulnerable to various types of attacks. Moreover, the network topological structure is dynamically configured due to higher mobility of self configured nodes. Security aspects in variety of application such as disaster, military application and entertainment industry have become a hot topic in the recent years since providing protection against various attacks is a very challenging task. The communication or routing in the wireless network among heterogeneous nodes is the main core in MANET however risky in terms of various vulnerabilities. The intruder node is very tough to distinguish from normal nodes in the network topology (Xing and Wang, 2010; Boppana and Su, 2011; Nadeem and Howarth, 2014; Komninos *et al*., 2007). Wireless networks are emerging in the context of node-to-node communication since mobile nodes can be easily deployed, doesn't incur physical connections and improves scalability. Moreover in mobile environment, routing plays a vital role in wireless communication (Wang *et al*., 2014; Xia *et al*., 2016; Liu *et al*., 2007).

Wireless medium encounters diverse transmission issues such as delay and packet drop which affect the network performance significantly. Furthermore, if the detection node is activated and it starts to consume bandwidth hence, it is desirable to activate only when it is needed. In particular, if some intruders are entered in the network which in turn it relays its own packet into the network. The attacker can affect Route Request (RREQ), Route Reply (RREP) and data packets by modifying few fields in the payload. Security attacks could bring severe damages especially where mobile devices are used to operate in dangerous environment or in critical scenarios. In this research, cooperative black hole attack is considered which affect the normal network operation by disrupting the routing process and attempts to consume the available bandwidth (Chang *et al*., 2015; Sanchez *et al*., 2015; Bu *et al*., 2011; Li *et al*., 2014; Xia *et al*., 2013). In literature, various techniques have been investigated to address these problems. Moreover,

Corresponding Author: T. Poongodi, Department of Computer Science and Engineering, PPG Institute of Technology, Tamil Nadu, India

bandwidth efficiency becomes a strong requirement to make assure mobile devices lifetime. Therefore, the proposed security technique intends at minimizing the routing overhead due to encryption.

AODV (Adhoc On-demand Distance Vector) is a reactive based routing protocol which involves two main processes: route discovery and route maintenance. In route discovery phase, the source node broadcasts a RREQ packet in the network. If an intermediate node has routing information to the destination in its routing table it replies with RREP to the source node. AODV does not have any detection mechanism; EBSR is presented that effectively detects the malicious nodes which try to launch collaborative black hole attacks. Black hole attack is an active routing attack where the malicious node announces it as the best node to reach all nodes in the network. The malicious node waits until neighboring nodes broadcasting RREQ packets. In particular, if the malicious node gets RREQ it starts transmitting a fake RREP with latest sequence number. The source node falsely believes that it is the best node for transmission of packets to the destination node. In this scheme, the packets for certain time interval are used for detecting malicious activities as well as malicious nodes which is sending false RREP messages and those nodes are detected using a tracing approach. The merit of this approach lies in statistical analysis of analytical and experimental results to achieve the fore mentioned goal.

Literature review: Zapata and Asokan (2002) proposed SAODV (Secure AODV) which uses digital signature for signing messages and hash value computation for securing hop counts, computational overhead is more in this technique which increases delay. Karlof and Wanger (2003) used multipath forwarding technique to identify attacks in wireless sensor network based selective forwarding attack procedure. The attackers are not detected and isolated from the network efficiently. Yu *et al.* (2010) applied secured technique based on the reputation evaluation in ad hoc networks. The behavior and correlation of the node is considered for building the reputation relation. This technique promotes the cooperation of cluster members while forwarding data packets.

Marti *et al.* (2000) proposed watchdog and pathrater mechanism which attempts to identify the misbehaving nodes in the network. When a node forwards a packet, the nodes watchdog verifies that the next node transmission in the path also forwards the packet. If next node does not forward the packet within the certain time limit it is assumed that the node is misbehaving. This mechanism suffers from false positive, node A may report that node B is not forwarding packets even though it is forwarding. Path Rater utilizes the knowledge of misbehaving nodes to select the network path for transmitting packets. Authentication mechanism (Sanzgiri *et al*, 2005) is proposed using public key cryptography based on AODV; however it mainly resists against only external attacks. Still there is a severe impact on the performance of the network due to some internal malicious activities launched by internal nodes.

Xiao *et al.* (2007) focused that intermediate nodes in the forwarding path are randomly selected as checkpoint nodes for sending acknowledgements for the received packets. If any misbehavior is detected, alarm packet is generated for transmitting information to the source node about the suspected activities. This scheme endures from huge overhead since of sending acknowledgement reverse to the source node for the entire received packets by intermediate nodes. Poongodi and Karthikeyan designed LSAM (Localized Secure Architecture for MANET) routing protocol to detect malicious nodes if the dynamic threshold is exceeded. If the sequence number is found abnormal and by discovering the shortest path where it is found based on link capacity computation. ALARM packet is sent to neighbours to inform about the suspected node and to move into the black list.

Wang *et al.* (2012) addressed the fault tolerance problem with Byzantine agreement. Eventual Byzantine agreement and Immediate Byzantine agreement are followed to obtain the common agreement at different rounds. Early dual agreement protocol is used to achieve the agreement by tolerating the maximum number of faulty processors and transmission media by utilizing only few number of message exchanges. This mechanism efficiently manages the network even if the processors move. Tamilselvan and Sankaranarayanan (2008) discussed about fidelity mechanism to prevent the cooperative black hole attack. Fidelity level is imputed for all actively participated nodes. If the level of any active node falls to 0, then the node is judged as malicious node and it is removed. Packet delivery ratio is better even in the presence of cooperative malicious nodes with minimum delay and overhead.

Banerjee (2008) used prelude and postlude messages for monitoring the data traffic. Prelude message is sent by the source node for alerting the destination node before sending data. The traffic is monitored by all intermediate nodes and at the end of data transmission; postlude message is used by the destination node to verify the count of received packets. The nodes exist around the source node turn into promiscuous mode to trace the data forwarding behavior even there is no attack which leads to energy consumption. Nakayama *et al.* (2009) proposed

a dynamic anomaly detection scheme for improving security against various attacks. Multidimensional features are defined to categorize an attack state from the normal state based on the features of attacks and PCA is used for finding the projection distance. This scheme significantly increases the detection rate and reduces the false positive rate against vulnerable activities.

Su (2011) focused on Anti Black Hole (ABM) mechanism which estimates the suspicious value of a node according to the amount of abnormal difference between RREQs and RREPs transmitted from the node. If an intermediate node is not the destination and never broadcasts a RREQ for a specific route but forwards a RREP for the route, then its suspicious value will be increased by 1 in the nearby IDS node's suspicious node table. When the suspicious value of a node exceeds a threshold, a Block message is broadcasted by the IDS node to all nodes in the network in order to isolate the suspicious node cooperatively. Wang *et al*. (2012) used trust based technique for enhancing the searching capability and scalability of the network. Cluster is formed by grouping nodes where nodes in the same cluster are bound closely depending on their trust relationship and share the same contextual information. Here the cooperation between two nodes is considered for computing the trust value.

MATERIALS AND METHODS

Proposed architecture: In general, proposed technique EBSR presents many challenges due to time varying delay and packet dropouts. The proposed methodology is investigated to detect an attack and mitigate its impact based on the concerned factors such as delivery ratio and delay. The proposed approach is embedded with cryptographic techniques to find an optimal solution. The asymmetric cryptographic technique is chosen to protect packets integrity, created signature is appended with the message during encryption process. Digital signature increases little overhead mainly due to the increased size of the packet which is to be transmitted.

Two issues considered are attack detection and attack mitigation. In the attack detection phase, detection mode is triggered only after the attack is detected and it avoids the unnecessary bandwidth consumption if the attack is not active. In the attack mitigation phase, once the attack is suspected action should be initiated which turns detection node into promiscuous listening, so that bandwidth consumption could be reduced and to maintain the on-going operation without any disruption.

Neighbor node communication: Usually neighbor nodes communicate only within a limited transmission range in the network. For an instance, node D wants to communicate with node C as shown in Fig. 1 but node C is not within the transmission range of D. Node D broadcasts RREQ that is received by node A and node E. Node E has no route to node C and therefore rebroadcasts to node D and in turn drops it. Node A has no route to node C and forwards to node B. As node B has a route to node C it replies to node A with RREP which in turn sends to node D. Hence, the route node D-Node A-Node B- Node C is confirmed for packet transmission.

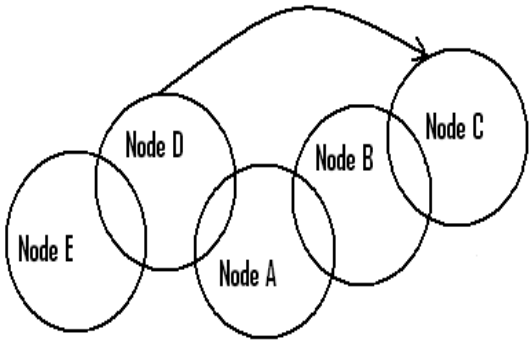

Fig. 1: Node communication

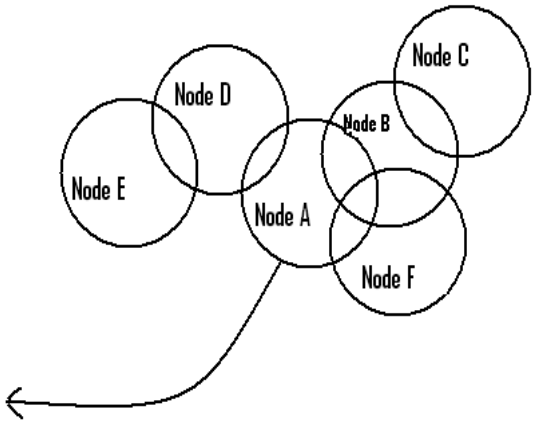

Fig. 2: Mobility scenario

Node F is in the communication range of Node A and Node B. As depicted in Fig. 2, node A moves out of the transmission range, node F detects it by not receiving Hello messages from Node A and marks the route as invalid. It sends RERR with invalid route to node B. Node B knows that Node A is not its neighbor.

According to mobility metric, α_i is determined dynamically by the number of neighboring nodes with the number of time slots $\Delta\tau_1 \ldots \Delta\tau_n$. For a given node i at time t, the network size can be changed relatively. α_i represents the change in the size of the network. The change in size

of network is defined by the change in the number of neighboring nodes. For an example, α_i for the first time slot is shown as Eq. 1:

$$\alpha_i = \frac{NSi(0) - NSi(1)}{N} + \frac{NSi(1) - NSi(0)}{N} \quad (1)$$

Where:

Nsi(0)-NSi(1) = The number of new neighbors at $\Delta\tau_n$

Nsi(1)-NSi(0) = The number of neighbors moved away at $\Delta\tau_n$

N = The total number of nodes participating in the network

Given the wireless ad hoc network α, the network survivability is denoted by $NS_i(\alpha)$ it is defined by all active nodes are connected.

Encryption and decryption: EBSR uses digital signature for signing routing messages only for selected packets which is not expensive like other existing techniques. Every node should have set of private and public keys for signing and verification. A network is framed, where the public keys are distributed within the transmission range. Let the network is represented as a graph GR = (V;E) be a network where V refers the set of vertices are nodes and E the set of edges are radio links among nodes. For each node p the set $N_i(p)$ which contains the vertices that are direct neighbors:

$$N_i(p) = \{ q : (p;q) \in E \text{ and } q \neq p \} \quad (2)$$

Likewise, to define the node $N_j(p)$ which has indirect neighbors of p:

$$N_j(p) = \{ r : (q;r) \in E \text{ and } q \in Ni(p), r \neq p \} \quad (3)$$

To define for n neighbor nodes of p[$N_n(p)$] with regard to $N_{n-1}(p)$ if the source node has n links to destination node. Initially, a node p has a private key $KY_{p,pnv}$ that is used for signing the selected packets of $N_i(p)$ and p's public key $KY_{p,pub}$ is distributed along with signed packets. Similarly a node q has an access to p's public key and the received encrypted packets are verified using $KY_{p,pub}$. Let S denotes the sender node and R the receiver node; $KY_{s,pnv}$, $KY_{s,pub}$ refers the private and public keys of node s respectively; ENCR(pckt, $KY_{s,pnv}$) represents the public key encryption algorithm on packet pckt of RREQ packet sent by the source node and the destination node has the public key $KY_{s,pub}$ are able to decrypt the packet using the sender's public key which has been already sent.

Anomaly detection: The overall processing of EBSR is depicted in Fig. 3. EBSR offers the possibility to attain the path information of malicious nodes and the legitimate nodes there by the trusted area can be easily identified by tracing RREP from malicious nodes. Additionally, the proposed scheme is capable of observing the malicious nodes activities and as a result, malicious nodes launching black hole attacks would be detected by EBSR. The intrusion detection system is activated only after the particular node crossing the threshold level. The baseline is introduced to identify the normal scenario and attack scenario of all the nodes in the network. Most of the existing approaches are not analyzing the content of the packets i.e., modified packets are not detected by those approaches. The proposed architecture aims at detecting the starting and ending time of the attack and defense against it. In particular, selective encryption is proposed for encrypting packets which is transmitted between the source node and the destination node.

It is preferred to guarantee the packet integrity and to reduce the bandwidth consumption in wireless network. The dynamic attack detection methodology is presented to compare the encrypted δ^e and unencrypted packets δ^{ue}.

Security verification: Selective encryption of packets are sent through the network not only to protect them in an efficient way but also to provide a way to detect an intrusion. By comparing the statistical report of two types of packets for certain period of time, attack is detected. The first one related to encrypted packets and the other related to unencrypted packets. Encrypted packets are collected in δ^{ue} and unencrypted packets are collected in δ^{ue}. The two kinds of packets are called as anchor packets, since they are always required by dynamic anomaly detection algorithm. The two time slots $\Delta\tau_1$ and $\Delta\tau_2$ are taken for sample whereas the packets in between indicated with or are sent. Figure 4 represents the case when no attack is detected (A = 0) while Fig. 5 represents the case when an attack is detected (A = 1). In normal scenario, (the attacker does not modify packet), the statistics of δ^e and δ^{ue} should be relatively nearer. In attacker scenario if the attacker modified the unencrypted packets, the two time series will be different.

Normal scenario and attack scenario: By considering all the time slots,

$$Ui = \{ \Delta\tau_1 \cup \Delta\tau_2 \cup \Delta\tau_3 \cup ..... \cup \Delta\tau_n \} \quad (4)$$

The incoming packets can be descended under anyone of the following categories, Scenario 1: δ^e refers the encrypted packets collected in the normal scenario and the sample data is collected for computation. Scenario 2: δ^{ue} refers the unencrypted packets collected in the normal scenario and the sample data is collected.

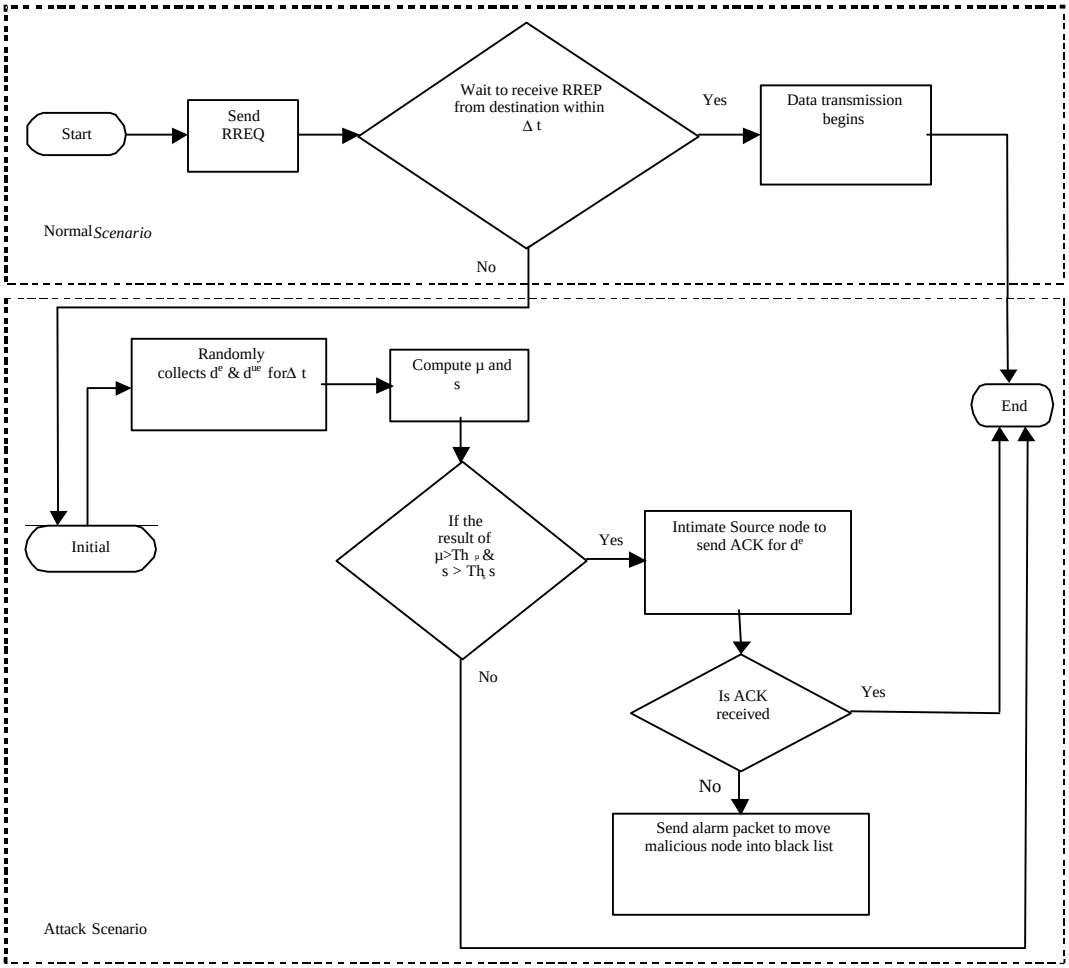

Fig. 3: Flow diagram of EBSR

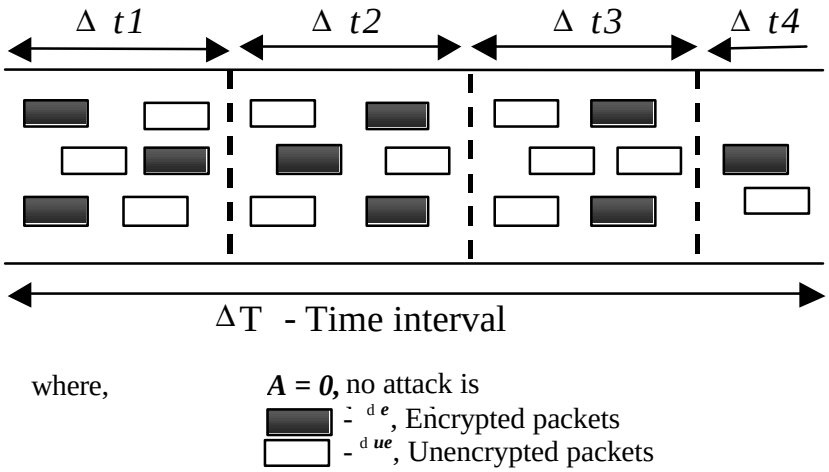

Fig. 4: Normal scenario

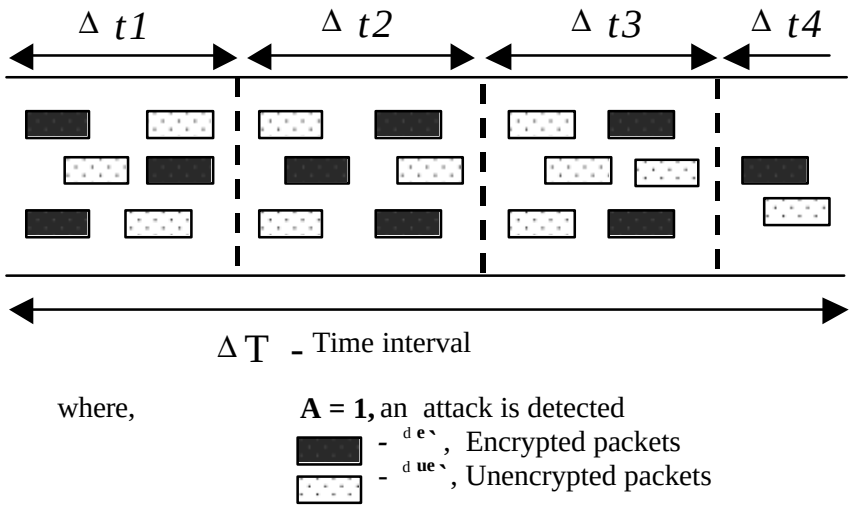

Fig. 5: Attack scenario

Scenario 3: $\delta^{e`}$ refers the encrypted packets collected in the attack scenario and the sample data is collected Scenario 4 : $\delta^{ue`}$ refers the unencrypted packets collected in the attack scenario and the sample data is collected. The entire process of EBSR for malicious node detection is briefly described in the form of procedure as given as.

Algorithm:

Procedure A = securityverification (δ^{e} $\delta^{ue}{}_{\Delta\tau 1 \ldots \Delta\tau n}$, $\delta^{e`}$ $\delta^{ue`}{}_{\Delta\tau 1 \ldots \Delta\tau n}$)

- To compute mean

μ_e=mean($U^{e}\Delta\tau 1 \ldots \Delta\tau n$)

μ_{ue}=mean($U^{ue}\Delta\tau 1 \ldots \Delta\tau 2_n$)

- To compute standard deviation

σ_e=std($U^{e}{}_{\Delta\tau 1 \ldots \Delta\tau n}$)

σ_{ue}=std($U^{ue}{}_{\Delta\tau 1 \ldots \Delta\tau n}$)

- Baseline verification on ì and ó

if $|\mu_e - \mu_{ue}| > Th_\mu$ OR $|\sigma_e - \sigma_{ue}| > Th_\sigma$ then

A=1 Attack detected

else

A=0 No attack

end if

end procedure

The recent work on the impact of packet drop fraction due to black hole attack shows that there is a need of severe security mechanisms. This finding recommends for further improvement of network performance by detecting and isolating the malicious nodes from the network. The proposed architecture has an extensive mechanism which defense against cooperative black hole attack.

RESULTS AND DISCUSSION

The network simulation tool (NS-2.34) is used to study the performance of EBSR scheme. The evaluation is based on the simulation of varying number of mobile nodes. MANET topology is constructed over a flat space of size (1000×1000 m) for 800 sec of simulated time. The Constant Bit Rate (CBR) data traffic sources with packet size of 64 bytes. Nodes in the simulation move accordingly to the random way point model with a speed of 2 m sec^{-1}. The pause time used in this simulation is varied from 10-50 sec.

Simulation parameters

Energy: It denotes the energy level in a node at a specific time. Each node will lose some amount of energy for transmitting and receiving packets. The energy consumption level of a node can be determined by taking the difference between current energy level and the initial energy level. The energy level of all nodes will be fixed with a maximum value. The energy will be utilized for a node to be in idle, sleep, transmit and receive modes. If the energy level reaches the minimum value then the particular node is not able to process any packets. The energy level should always be maintained between E_{min} and E_{max}. The total energy level can be calculated by taking the difference of E_i, E_c for entire node's energy level. The consumed amount of energy level can be computed as:

$$E = \sum_{k=0}^{n} E_c - E_i \quad (5)$$

Where:

E_i, E_c = The initial energy level of a node and the current energy level of a node

E_{max}, E_{min} = The maximum energy level of a node and the minimum energy level of a node

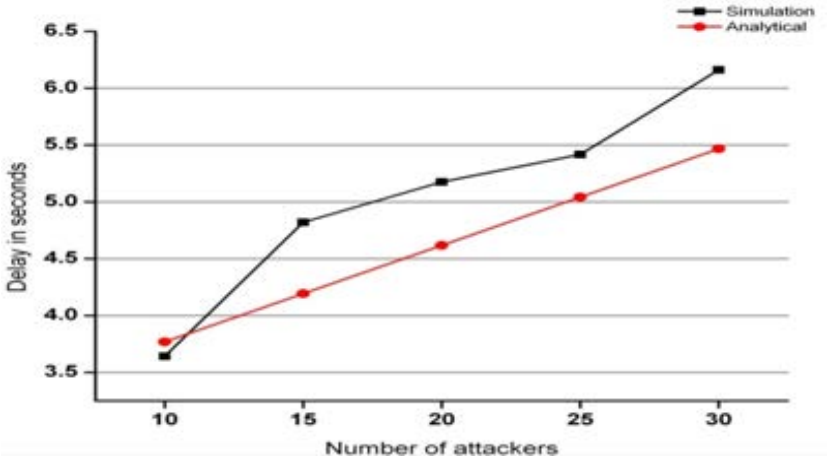

Fig. 6: Delay-analytical vs. simulation

False positive: In a certain period, the source node detects the attack when there is no attacker even the attack is failed. It is the frequency with which the detection node falsely reports the occurrence of malicious activity. The false positive (fp) is denoted as,

$$fp = \neg\gamma_s \wedge \gamma_d \quad (6)$$

where $\neg \gamma_s$, γ_d denotes that the attack is not succeeded and the attack is detected.

False negative: It occurs when the node doesn't detect while actually there are attackers. It is the frequency where the detection node fails to report when malicious activity actually occurs. The false negative (fn) is denoted as:

$$fn = \gamma_s \wedge \neg\gamma_d \quad (7)$$

Where γ_s, $\neg \gamma_d$ represents that the attack is succeeded and the attack is not detected.

Delay: A data packet takes certain time to arrive in the destination. The delay includes the route identification process and the time taken for the packets in transmission. The elapsed time is defined as by taking the difference from starting time to arrival time. Delay (D) can be calculated as:

$$D = \sum_{k=1}^{n} T_s - T_a / \Delta\tau_n \quad (8)$$

Where T_s, T_a refers the starting time and the arrival time of data packet transmission.

PDR: The packet delivery ratio is defined as the ratio of the total number of packets received (P_r) to the total number of packets sent (P_s) in a particular session. It is denoted as:

$$PDR = \sum_{k=1}^{n} P_r / P_s \quad (9)$$

Where P_r, P_s denotes the number of packets received and the number of packets sent.

Performance analysis: Only authentic users in the secured environment are able to use the network resources and the compromised nodes will be excluded for further communication. The intruder injects packets into the network to consume valuable network resources such as band width or to consume node resources such as memory or computational power. The malicious nodes consume more energy, decrease path availability and increase travel time of packets by loading irrelevant packets into the network. Those nodes have to be detected, so there is a need for a technique to detect and eliminate it. This problem can be handled by EBSR to prevent energy consumption using selective encryption method. In experimental analysis, the number of attackers is varied and the results are obtained by comparing the proposed protocol EBSR with the base protocols SAODV and LSAM. The proposed protocol is examined based on analytical and simulation results.

The comparison of analytical and simulation results of attackers vs delay for EBSR protocol is shown in Fig. 6. Delay slowly increases as the number of attackers increase. The analytical results for the delivery ratio are

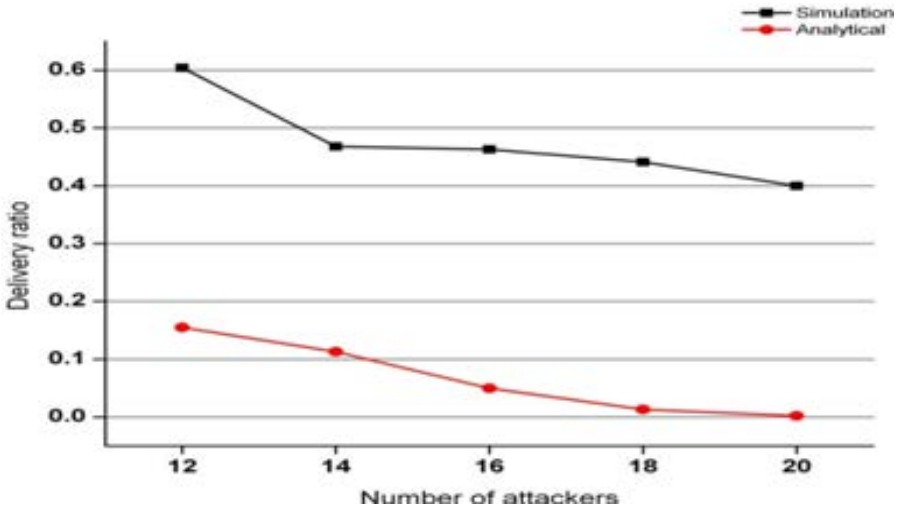

Fig. 7: PDR-analytical vs. simulation

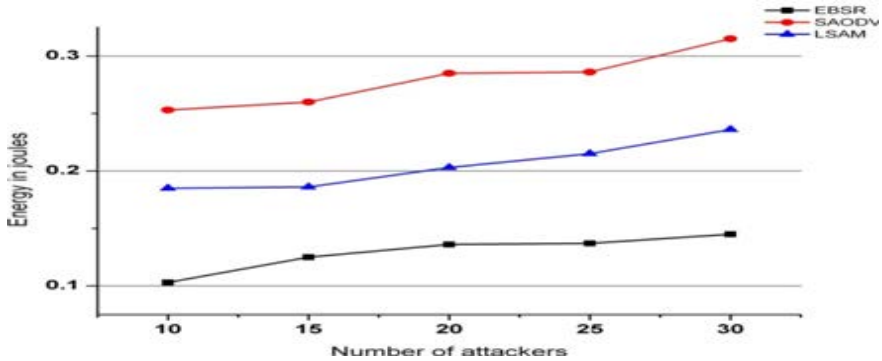

Fig. 8: Energy vs. number of attackers

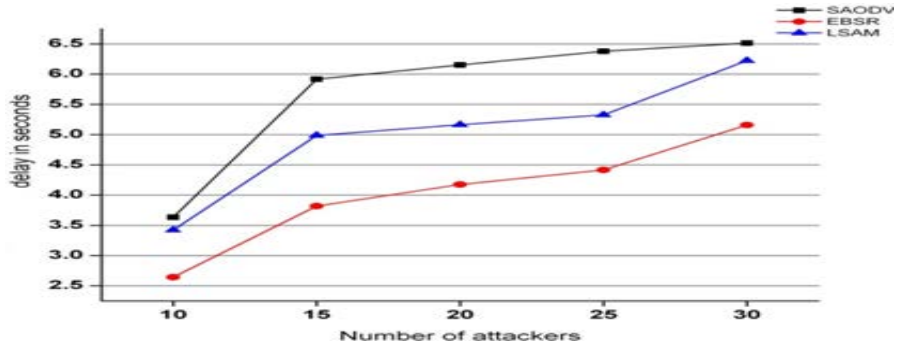

Fig. 9: Delay vs. number of attackers

obtained and it is compared with the simulation results to show its performance. The analytical and simulation results of packet delivery ratio for the misbehaving nodes 12, 14, 16, 18 and 20 are shown in Fig. 7. It can be seen that both analytical and simulation results converges with significant difference. The delivery ratio slowly decreases as the number of attackers increase. Figure 8 shows the results of attackers vs energy for EBSR protocol in comparison with SAODV protocol and LSAM protocols in the form of a graph. It can be seen that as the number of attackers increase, the energy level of the EBSR increases compared to SAODV and LSAM protocols.

It can be seen from Fig. 9 that as the number of attackers increase, the EBSR slows down in time but the SAODV and LSAM protocols retains the minimum delay advance. As the possibility of attackers' increases, EBSR

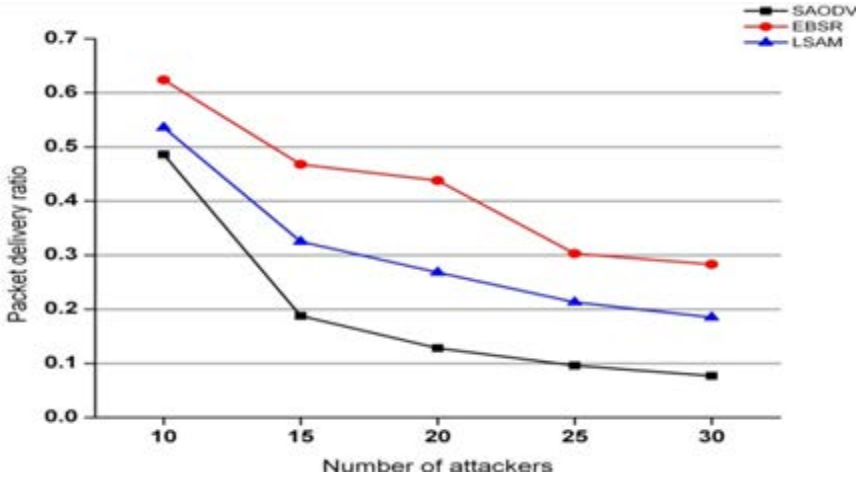

Fig. 10: PDR vs. number of attackers

is more efficient as it eliminates the time loss. The results of attackers vs delay for EBSR in comparison with SAODV and LSAM protocols in the form of a graph.

If the number of attackers increases, the EBSR delivers the packets quickly but the SAODV and LSAM protocols delays in delivering the packets. Figure 10 shows the results of attackers Vs delivery Ratio for EBSR in comparison with SAODV protocol and LSAM protocols in the form of a graph.

CONCLUSION

In this study, a light weight EBSR is proposed for detecting malicious nodes in the network under cooperative black hole attacks. The proposed protocol could be integrated with the exiting routing protocols for MANET such as AODV and DSR. The computation at each node is still a major issue, hence the analytical investigation is made and it is compared with simulation results. By considering the mobility, the network size is determined for certain time interval and the performance is analyzed. In this formulation, attack detection and mitigation share the information gathered analytically and experimentally. The simulation results were presented to show the significance performance improvement in all the taken performance metrics. The proposed methodology shows an effective performance in terms of reducing the false positive and false negative rate against the cooperative black hole attack.

REFERENCES

Banerjee, S., 2008. Detection removal of cooperative black and gray hole attack in mobile ad-hoc networks. Proceedings of the World Congress on Engineering and Computer Science WCECS, October 22-24, 2008, RCC Institute of Information Technology, San Francisco, USA, ISBN: 978-988-98671-0-2,-pp: 22.

Boppana, R.V. and X. Su, 2011. On the effectiveness of monitoring for intrusion detection in mobile ad hoc networks. IEEE. Trans. Mob. Comput., 10: 1162-1174.

Bu, S., F.R. Yu, X.P. Liu and H. Tang, 2011. Structural results for combined continuous user authentication and intrusion detection in high security mobile ad-hoc networks. IEEE. Trans. Wirel. Commun., 10: 3064-3073.

Chang, J.M., P.C. Tsou, I. Woungang, H.C. Chao and C.F. Lai, 2015. Defending against collaborative attacks by malicious nodes in MANETs: A cooperative bait detection approach. IEEE Syst. J., 9: 65-75.

Karlof, C. and D. Wagner, 2003. Secure routing in wireless sensor networks: Attacks and countermeasures. Ad Hoc Networks, 1: 293-315.

Komninos, N., D. Vergados and C. Douligeris, 2007. Detecting unauthorized and compromised nodes in mobile ad hoc networks. Ad Hoc Networks, 5: 289-298.

Li, T., M. Abdelhakim and J. Ren, 2014. N-Hop networks: A general framework for wireless systems. IEEE. Wirel. Commun., 21: 98-105.

Liu, K., J. Deng, P.K. Varshney and K. Balakrishnan, 2007. An acknowledgment-based approach for the detection of routing misbehavior in MANETs. IEEE Trans. Mobile Comput., 6: 536-550.

Marti, S., T.J. Giuli, K. Lai and M. Baker, 2000. Mitigating routing misbehavior in mobile ad hoc networks. Proceedings of the 6th Annual ACM/IEEE International Conference on Mobile Computing and Networking, August 6-11, 2000, Boston, MA., USA., pp: 255-265.

Nadeem, A. and M.P. Howarth, 2014. An intrusion detection and adaptive response mechanism for MANETs. Ad Hoc Netw., 13: 368-380.

Nakayama, H., S. Kurosawa, A. Jamalipour, Y. Nemoto and N. Kato, 2009. A dynamic anomaly detection scheme for AODV-based mobile ad hoc networks. IEEE Trans. Vehicular Technol., 58: 2471-2481.

Sanchez, C.L., M.G. Fernandez, G.P. Teodoro and M.R. Carrion, 2015. A model of data forwarding in MANETs for lightweight detection of malicious packet dropping. Comput. Netw., 87: 44-58.

Sanzgiri, K., D. LaFlamme, B. Dahill, B. Levine, C. Shields and E.M. Belding-Royer, 2005. Authenticated routing for ad hoc networks. IEEE J. Sel. Areas Commun., 23: 598-610.

Su, M.Y., 2011. Prevention of selective black hole attacks on mobile ad hoc networks through intrusion detection systems. Comp. Commun., 34: 107-117.

Tamilselvan, L. and V. Sankaranarayanan, 2008. Prevention of co-operative black hole attack in MANET. J. Networks, 3: 13-20.

Wang, B., X. Chen and W. Chang, 2014. A light-weight trust-based QoS routing algorithm for ad hoc networks. Pervasive Mob. Comput., 13: 164-180.

Wang, W., G. Zeng, J. Yao, H. Wang and D. Tang, 2012. Towards reliable self-clustering mobile ad hoc networks. Comput. Electr. Eng., 38: 551-562.

Xia, H., J. Yu, C.L. Tian, Z.K. Pan and E. Sha, 2016. Light-weight trust-enhanced on-demand multi-path routing in mobile ad hoc networks. J. Netw. Comput. Appl., 62: 112-127.

Xia, H., Z. Jia, X. Li, L. Ju and E.H.M. Sha, 2013. Trust prediction and trust-based source routing in mobile ad hoc networks. Ad Hoc Netw., 11: 2096-2114.

Xiao, B., B. Yu and C. Gao, 2007. CHEMAS: Identify suspect nodes in selective forwarding attacks. J. Parallel Distrib. Comput., 67: 1218-1230.

Xing, F. and W. Wang, 2010. On the survivability of wireless ad hoc networks with node misbehaviors and failures. IEEE. Trans. Dependable Secure Comput., 7: 284-299.

Yu, Y., L. Guo, X. Wang and C. Liu, 2010. Routing security scheme based on reputation evaluation in hierarchical ad hoc networks. Comput. Netw., 54: 1460-1469.

Zapata, M.G. and N. Asokan, 2002. Securing ad hoc routing protocols. Proceedings of the 1st ACM Workshop on Wireless Security, September 28, 2002, Atlanta, GA., USA., pp: 1-10.