Journal of Computer Science, 9 (1): 105-113, 2013
ISSN 1549-3636

doi:10.3844/jcssp.2013.105.113 Published Online 9 (1) 2013 (http://www.thescipub.com/jcs.toc)

FLOODING ATTACK AWARE SECURE AODV

Madhavi, S. and K. Duraiswamy

Department of Computer Science and Engineering,
K.S. Rangasamy College of Technology, Namakkal, Tamil Nadu, India

Received 2012-07-18, Revised 2012-07-19; Accepted 2013-02-27

ABSTRACT

Providing security in a Mobile Ad hoc Network (MANET) is a challenging task due to its inherent nature. Flooding is a type of Denial of Service (DoS) attack in MANET. Intentional flooding may lead to disturbances in the networking operation. This kind of attack consumes battery power, storage space and bandwidth. Flooding the excessive number of packets may degrade the performance of the network. This study considers hello flooding attack. As the hello packets are continuously flooded by the malicious node, the neighbor node is not able to process other packets. The functioning of the legitimate node is diverted and destroys the networking operation. Absence of hello packet during the periodical hello interval may lead to wrong assumption that the neighbor node has moved away. So one of the intermediate neighbor nodes sends Route Error (RERR) message and the source node reinitiates the route discovery process. In a random fashion the hello interval values are changed and convey this information to other nodes in the network in a secured manner. This study identifies and prevents the flooding attack. This methodology considers the performance parameters such as packet delivery ratio, delay and throughput. This algorithm is implemented in Secure AODV and tested in ad hoc environment. The result of the proposed algorithm decreases the control overhead by 2%.

Keywords: Hello Packet, Flooding, MANET, Malicious Node

1. INTRODUCTION

The mobility of the nodes in MANET and the wireless links established between the nodes are vulnerable to various types of attacks. Mobile node and wireless link is the main component of wireless network. The characteristics of the MANET is categorized based on above mentioned component. Free mobility, constrained resources, poor physical protection and self organization are the characteristics expressed by the mobile node. Limited bandwidth and open transmission medium are the uniqueness explored by wireless link. Such a uniqueness of MANET exploits the vulnerabilities is substantiated in **Fig. 1**.

The inherent nature of MANET is susceptible to different kinds of attacks. One of them is DoS attack which includes Black hole, wormhole and flooding. DoS attackers aim is to increase the packet loss, delay, more usage of bandwidth and decrease the throughput. In a black hole attack, the node sends fake Route Reply (RREP) to the source. During the data transmission, the node drops the packet without forwarding. More than one attacker node is involved in wormhole creation. Attacker node tunnels the packet to other attacker location and replay the packet from there.

Flooding, where a message from a source is delivered to all other nodes, has extensive applicability in ad hoc wireless networks (Lim and Kim, 2001). For example, several point-to-point routing algorithms such as AODV and DSR rely on flooding to obtain routing information. Flooding is a type of DoS attack, but it may flood either the control or data packet continuously. It creates a lot of damage in the network. It consumes more power, bandwidth and resources. During the route discovery process either it may flood RREQ or RREP packets.

In this attack the source may act as malicious node. If any one of the malicious node intent to disrupt either the network operations or other node's activity in the network, the malicious node initiates the route discovery process.

Corresponding Author: Madhavi, S., Department of Computer Science and Engineering, K.S. Rangasamy College of Technology, Namakkal, Tamil Nadu, India

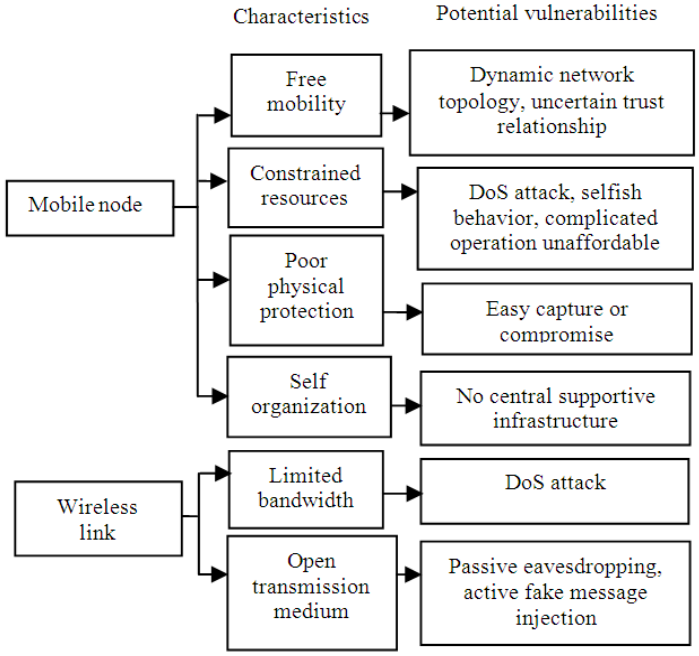

Fig. 1. Characteristics and vulnerabilities of MANET

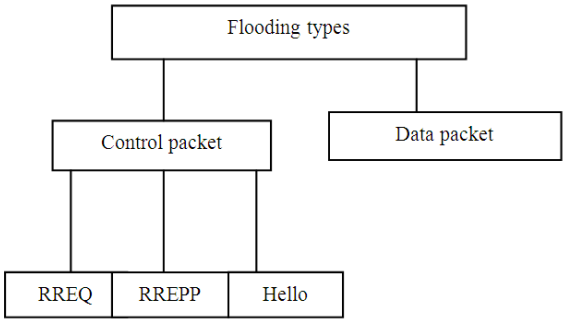

Fig. 2. Flooding attack types

It tries to find the path for some anonymous or unavailable node in the network. So the malicious node floods the RREQ packet in infinite times. Other participated nodes are unable to handle other packets which are received by them. Due to the flooding of RREQ, the intermediate cannot concentrate on other activities like forwarding. Hysterical rainfall causes flood. It affects normal activities of day to day life. In a similar manner the flooding of either control or data packets affect the network operation. Flooding attacks are classified into two types namely control packet flooding and data packet flooding which are shown in **Fig. 2**. Flooding of RREQ, RREP and Hello packets are the examples of control packet.

A control packet flooding is a DoS attack in which malicious node takes advantage of either route discovery process or to maintain a local connectivity between the nodes. In the route discovery process either it floods the RREQ or RREP packets. So overflow of the routing table in the intermediate node is the effect of this malicious activity. Hello flood is one of the active attacks (Hamid *et al*., 2006). If the malicious node floods the hello packet unnecessarily, neighbors of the malicious node cannot receive other packets. In general, it results in congestion, exhaustion of battery power, wastages of bandwidth and degrades the throughput.

1.1. Related Work

Review the prior work of flooding attack and its countermeasures are carried out for the present work.

This study (Williams and Comp, 2002) categorizes the flooding schemes into the following five proposed groups based on the AODV routing protocol in MANET:

- Probabilistic scheme-when receiving a broadcast message for the first time, a host rebroadcasts the message with a fixed probability P

- Counter-Based scheme: It inhibits the rebroadcast if the message has already been received for more than C times
- Distance-Based scheme: This scheme, a node rebroadcasts the message only if the distance between the sender and the receiver is larger than a threshold D
- Location-Based scheme: It rebroadcasts the message if the additional coverage due to the new emission is larger than a bound A
- Cluster-Based scheme: It uses a cluster selection algorithm to create the clusters and then the rebroadcast is done by head clusters and gateways

This study is based on rate based model. It introduced a (Silva, 2004) simple rate-based control packet forwarding mechanisms to mitigate malicious control packet floods. This study identified the flooding attack based on the behavior of the node (Guo and Simon, 2010). It presented a behavior-based trace back mechanisms to identify flooding attack origin and an attack isolation scheme to alleviate the impact on the network. There are spoofing and non spoofing attacks are dealt with this study. Flow based detection features are used for detecting flooding attack.

It filters the misbehave node using two threshold value RATE_LIMIT and BLACKLIST_LIMIT (Song *et al*., 2006). It handles RREQ flooding attack. The RATE_LIMIT denotes the number of RREQ, if the number of packet reception times is less than or equal the RATE_LIMIT, it can be accepted and processed by a node. BLACK_LIST_LIMIT can identify the misbehaving node, if the packet originated by a node exceed the per unit time.

It used a mechanism Route Request Flooding Attack (RRFA) to detect and prevent the flooding attack (Eu and Seah, 2006). They consider RREQ flooding for their work. In this, RREQ flooding attack classified into two types, depth RRFA and breath RRFA. In breath RRFA, the attacker node is initiated route discovery to the unreachable destination. It can be implemented at two levels of protocol stack such as application and network layers. Depth RRFA consider only one unreachable destination node and attacker would generate the large number of RREQ. This methodology is named as Route Request Flooding Defense (RRFD). It consists of three components such as RREQ binary exponential backoff, Route Discovery Cycle (RDC) binary exponential backoff and Fast Recovery.

This study suggested three threshold values to identify and isolate the flooder node in the network (Balakrishnan and Varadharajan, 2005). This methodology maintains two lists such as white and black list threshold. In their analysis the flooding attacks are mitigated nearest to the source of attack.

The author used the extended DSR protocol based on the trust function to mitigate the effects of flooding attack (Theodorakopoulos and Baras, 2006). In this study, based on the trust value they categorized the nodes in three categories: Friends, acquaintance and stranger. Stranger are the non trusted node, friends are the trusted node and acquaintance has the trust values more than stranger and less than friends. Based on relationship they define the three threshold value. If any node receives the RREQ packets then checks the relationship and based on that it checks for the threshold value if it is less than the threshold then forward the packet otherwise discard the packet and blacklist the neighbor node. The main problem with this method is not work well with higher node mobility.

This study proposed a methodology to detect and prevent the flooding attack using signal strength and client puzzle method (Singh *et al*., 2010). The received signal strength is compared with the fixed threshold value, if it is smaller value, the sending node categorized as intruder otherwise it sends the puzzle for that node, if the receiving node sends correct answer, categorized as normal otherwise moved to intruder category.

2. MATERIALS AND METHODS

In MANET, routing protocols are classified as reactive, proactive and hybrid. This study considers reactive routing protocol, specifically extension of AODV for security purpose. The reactive routing protocols consist of series of actions from either the source to the destination nodes or intermediate node who knows a route to the destination. The reactive routing protocol consists of two different phases such as route discovery and data transmission. For example, route discovery process includes sequence of actions like (1) The source node delivers an initial Route Request; (2) Each node (except for the source node and the node that has a route to the destination) in the forward path receives a Route Request from the previous node and forwards it; (3) The replying node receives the Route Request and replies with a Route Reply message; 4) An intermediate node in the reverse path receives a Route Reply message and forwards it.

Secure AODV (SAODV) is similar to AODV but it uses cryptographic mechanisms for providing a security in a reactive routing protocol (Guerrero-Zapata and Asokan, 2002).

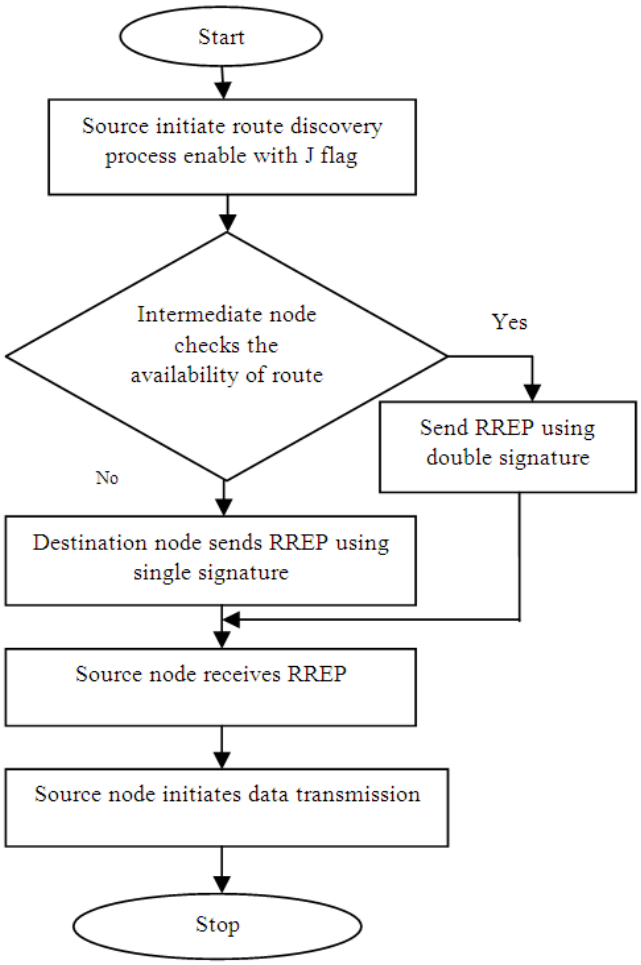

Fig. 3. Steps in SAODV

SAODV provides security for mutable and non-mutable part of the packet content. Even though, there is a possibility of insider attacks, such as rushing/tunneling attacks and Medium Access Control (MAC) layer misbehavior (Mulert *et al*., 2012). Misbehaving participated nodes in the network are called as Insider attacker. The SAODV protocol was not designed to withstand DoS attacks. This study deals with DOS attacks specifically for flooding attack. **Figure 3** shows the processing sequence of SAODV. SAODV is a security extension of the AODV protocol, based on public key cryptography. SAODV routing messages are digitally signed to guarantee their integrity and authenticity (Guerrero, 2001). Therefore, a node that generates a routing message signs it with its private key and the nodes that receive this message verify the signature using the sender's public key.

The hop count cannot be signed by the sender, because it must be incremented at every hop. Therefore, to protect it a mechanism based on hash chains is used. In its basic form, this makes it impossible for intermediate nodes to reply to RREQs if they have a route towards the destination, because the RREP message must be signed by the destination node.

To preserve the collaboration mechanism of AODV (Perkins and Royer, 1999), SAODV includes a kind of delegation feature that allows intermediate nodes to reply to RREQ messages. This is called the double signature. When a node A generates a RREQ message, in addition to the regular signature, it can include a second signature, which is computed on a fictitious RREP message towards a itself. Intermediate nodes can store this second signature in their routing table, along with other routing information related to node A. If one of

these nodes then receives a RREQ towards node A, it can reply on behalf of A with a RREP message, similarly to what happens with regular AODV. To do so, the intermediate node generates the RREP message, includes the signature of node A that it previously cached and signs the message with its own private key.

SAODV utilizes hash chains to keep the integrity of distance information, namely the hop count field, which is supposed to be incremented at each hop. This mechanism basically works as follows. When a node generates a RREQ or RREP message, it performs the following actions:

- Generate a random number called seed
- Set the maximum hop count field, dm, to TTL value from
- The IP header. This is practically the expected diameter
- Of the network
- Initialize the hop count field, *d*, to zero
- Initialize the hash field, h, to seed
- Calculate top hash field, htop, by hashing seed dmax times

When a node receives a RREQ or RREP, it performs the following actions:

- Verify the hop count field, d, by applying hash function to the current hash field times if the result equals htop, i.e., d is VERIFIED if H(dmax¡d)(h) = htop
- If the message is to be re-broadcast, increment d and apply the hash function to h and store the result back note that the top hash field (htop) is immutable and therefore it is included in the signature generated by the message initiator. This ensures the integrity of the field

During this process nodes in the network will maintain local connectivity between them using HELLO packet. A node determines connectivity information by listening hello messages from its set of neighbors. A node should use hello messages only if it is part of active route.

2.1. Hello Message and its Operations

Hello message is a RREP message with TTL = 1. It is also signed like RREP. But hello intervals are not signed because other than the active route nodes that are available in the network, they are unable to receive this message. Hello packet with following fields:

- Destination IP address
- Destination Sequence Number
- Hop Count
- Lifetime

Lifetime value is determined by two variables: ALLOWED_HELLO_LOSS and HELLO_INTERVAL that controls the connectivity of the neighbors. HELLO_INTERVAL is the time interval between hello message transmissions. ALLOWED_HELLO_LOSS is the maximum number of periods of HELLO_INTERVAL to wait without receiving a hello message before it detects loss of connectivity with its neighbors. Value of HELLO_INTERVAL is 1 sec. and ALLOWED_HELLO_LOSS is 3 packets.

Each node maintains neighbor table for keeping local connectivity information about its neighbors. Whenever node receives hello message from its set of neighbors, it checks the route to that neighbor node exists in a neighbor table. It updates route information by updating lifetime of that neighbors by ALLOWED_HELLO_LOSS * HELLO_INTERVAL otherwise the node makes the entry for that route in neighbor table. After making entry of that route current node can use this route to forward the data packets. Routes that are created by hello messages are not used by other active routes and do not generate a RERR message if neighbor node moves away and a neighbor timeout occurs.

Hello message transmission is between the neighbors nodes in the network are shown in **Fig. 4**. Hello messages have a bidirectional link. In the absence of this message with a certain interval, it assumes the neighbor node is moved away from this network. It sends the route error message. Nodes will respond to the HELLO message to maintain the local connectivity. In a HELLO flood attack, the malicious node sends number hello packets without considering the hello interval. It reduces the time interval and sending more number of hello packets to its neighbor and distracted the work of the other nodes in the network. Even though, SAODV is a secured protocol it suffered from inside attackers.

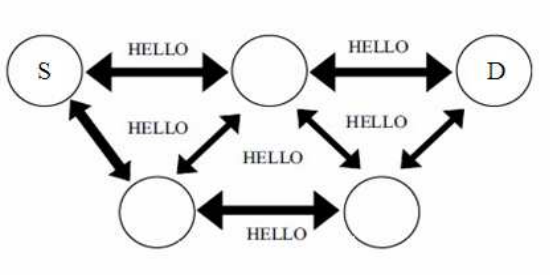

Fig. 4. Hello message transmission

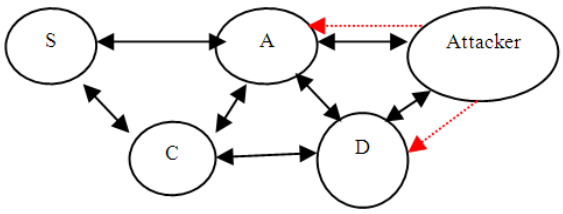

Fig. 5. Hello flooding attack

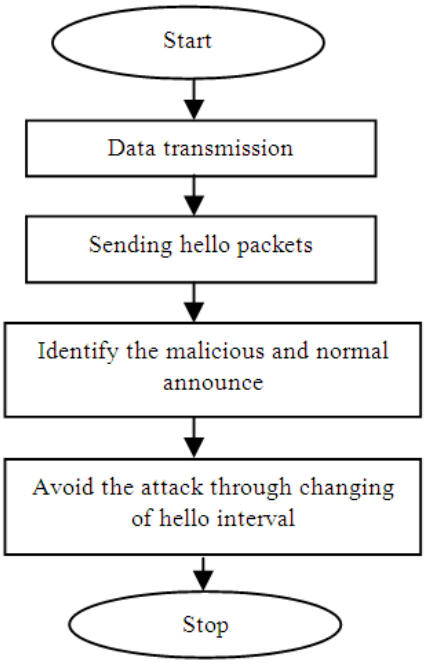

Fig. 6. General process of FAA-SAODV

Flooding Attack Aware SAODV (FAA-SAODV) provides a solution for the hello flooding attack. This algorithm is slightly modified from SAODV. After the transmission of RREQ packet, nodes are initiated to send Hello packet to its neighbor. Generally the hello interval changed in a random fashion but it limits between the maximum and minimum hello interval values. FAA-SAODV, initially all nodes are acting as a normal node. After very short time duration the malicious sends the hello packet continuously without considering the interval.

2.2. FAA-SAODV

Main objective of this study is to identify the flooder attacker and prevention mechanisms. Maintain a local connectivity is a important task. Some misbehaving nodes in the network flood the Hello packet continuously without maintaining the hello interval. It creates the disturbances in the network operation. This activity diverts the legitimate node's action in the network. **Figure 5** shows the hello flooding in the network.

In this method assumes, hello interval values are changed in a random manner. This value is encrypted and attached in the header part of the data packet. Nodes that are located in the coverage area, are able to process the header part of the packet and update this hello interval value and changing the time of sending hello packets its neighbor. But the malicious won't concentrate the processing of other packets, it continuously sends large number hello packets to its neighbor. It is unaware of these changes of hello interval.

FAA-SAODV identify and prevent from this hello flooding attack is based on their relationship with the neighboring node. It is categorized as normal and malicious nodes. The random hello intervals are used to identify the flooder. Malicious nodes are not aware of this change of hello interval, so it does not change the interval and continuously send the packet to its neighbor. This behavior exhibits the confirmation of malicious activity and the neighbor node ignores the processing of packets. **Figure 5** shows the general process of FAA-SAODV. Red lines are indicating the malicious action of the attacker node. The nodes A and D unable process the continuous hello packets so it is indicated as unidirectional.

FAA-SAODV is used to identify a malicious node based on two step process. Initially all the nodes in the network agreed to send a hello packet in a fixed interval. The first step is an analysis of the time duration of received hello packets. Node which has a variation in the fixed interval will be assumed as a normal node. Then it performs the second step for taking decision either a normal or a malicious. Calculation of allowed hello loss is also varying based on the hello interval.

2.3. Malicious Node

The strangers are the unbelievable node. Initially when any node joins the network, then this trust relationship with its all the neighbors are low or negligible that node is treated as stranger or malicious.

2.4. Normal Node

Friends are most believable nodes, based on the random hello interval. These types of nodes are not used to fix hello interval value. Random hello interval value is greater compared to fixed value. Here the highest believable node is mean usage of the randomly changed interval values. The **Fig. 6** shows the identification of the nodes during the hello packet transmission.

The following steps are illustrated the process of FAA-SAODV:

- Source node initiates route discovery process
- Intermediate node ensures the authenticity and integrity
- If the intermediate has a fresh enough route, it sends the gratitude RREP to the source. Otherwise forward packet to next level
- Source node receives the RREP, it unicast the data packets
- Initiate to send hello packets to maintain local connectivity
- Malicious node is floods the hello packet either without waiting the interval between the hello packets or not using the randomly changing the hello interval and it uses fixed 1msec as hello interval
- Every node in the network calculates the receiving time of the hello packets. If receiving hello interval is less than the current random hello interval, the node will be considered as malicious otherwise treated as normal node
- The neighbor node is removing the entry of the malicious from its routing table and packet is not processed when it is send by malicious
- Randomly changed hello interval value is attached in the header part of the data packet. The header part is processed by all the nodes which are located in a transmission range other than active route member

3. RESULTS AND DISCUSSION

NS-2 simulator is used for this simulation study. This study considers three cases such as SAODV, Att-SAODV and FAA-SAODV. In the sample scenarios, Traffic source is Constant-Bit-Rate (CBR) and the field configuration is 800×800 m with varying number of nodes from 50 to 100. **Table 1** shows the simulation settings of the simulation. Three different cases are considered for this simulation. The first and second cases are examines the performance of SAODV with and without attacker. The third case assesses the performance of FAA-SAODV with attacker.

This simulation evaluates the control over head, throughput and packet delivery ratio. **Figure 7** compares the control over head of the two routing protocols with fixed node speed with varying number of nodes. FAA-SAODV includes both legitimate and malicious nodes. Control over head of SAODV is 17% and Att-SAODV is 18%. FAA-SAODV is 16%. It decreases the control over head by 2% with the presence of attackers.

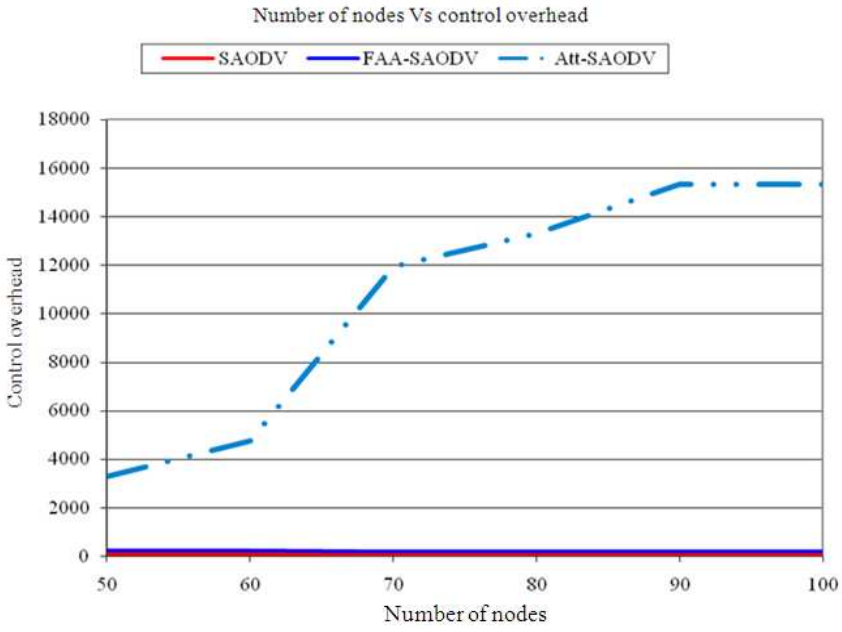

Fig. 7. Number of nodes Vs Control Over Head

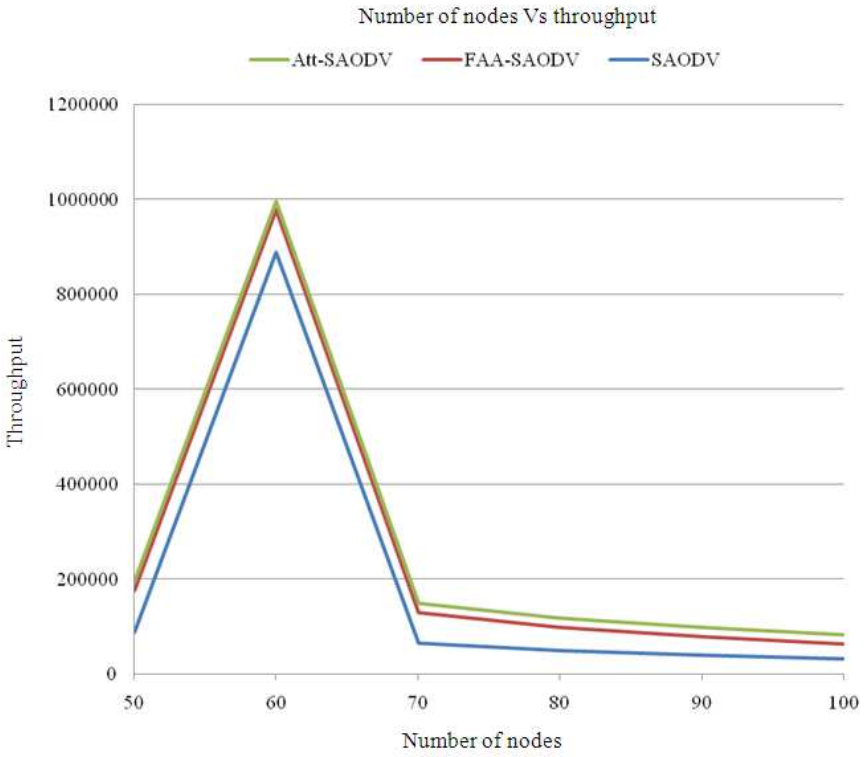

Fig. 8. Number of nodes Vs Throughput

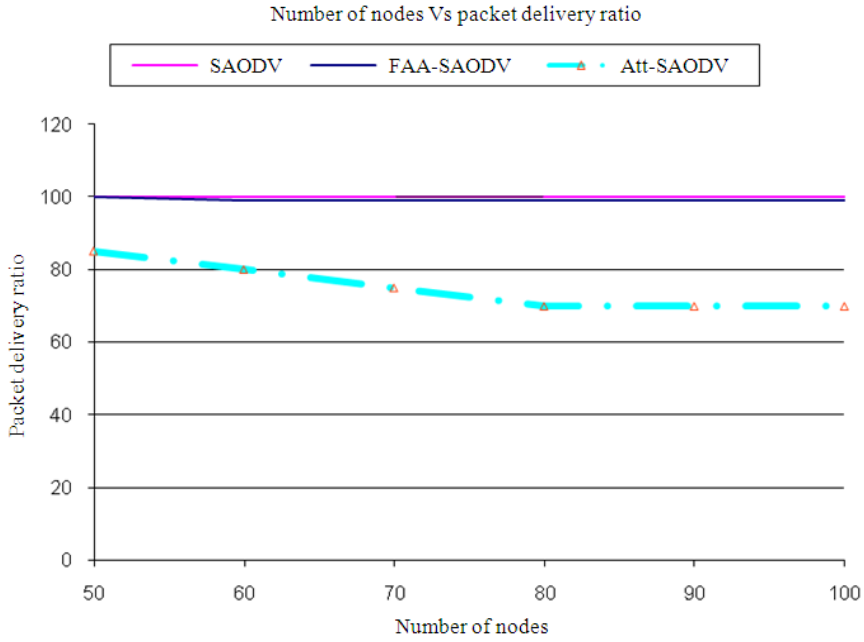

Fig. 9. Number of Nodes Vs PDR

Table 1. Simulation settings

Parameters	Values
Topology size	800×800
Communication traffic	CBR
Varying number of nodes	50, 60, 70, 80, 90, 100
Speed	0.5 m/sec
Mobility model	Random way point
Pause time	10 sec
Data transfer rate	512 kbps
Total simulation time	200 seconds
Attacker nodes	23, 43, 11

Figure 8 shows the throughput of SAODV, FAA-SAODV and Att-SAODV. Presence of the attacker, SAODV achieves little bit higher throughput.

Figure 9 shows the packet delivery ratio of SAODV and FAA-SAODV. SAODV achieves 100% PDR without the presence of attacker. FAA-SAODV performance is better with the presence of attacker. It achieves 99% PDR. Att-SAODV is produces 75% PDR. Presence of attackers in SAODV-att, the Packet delivery ratio is reduced 25% in SAODV and for FAA-SAODV is 24%.

4. CONCLUSION

This simulation work evaluates the performance of SAODV and FAA-SAODV. FAA-SAODV is tested with the presence of flooding attackers. Three performance parameters are considered. FAA-SAODV, control over head is increased when compared with SAODV because of the presence of attacker. Other two parameters namely PDR and throughput also show little bit improvement. The result obtained in the present work is pertaining to the presence of only one kind attack that is flooding attack. Presence of more than one kind of attacker may affect the performance of the network. Further work is required in this line.

5. REFERENCES

Balakrishnan, .V and V. Varadharajan, 2005. Fellowship in mobile ad hoc networks. Proceedings of IEEE Security and Privacy in Emerging Areas, (SPEA' 05), Athens, Greece.

Eu, Z.A. and W.K.G. Seah, 2006. Mitigating route request flooding attacks in mobile ad hoc networks. Proceedings of the International Conference on Information Networking: Advances in Data Communications and Wireless Networks, Jan. 16-19, Springer Berlin Heidelberg, Sendai, Japan, pp: 327-336. DOI: 10.1007/11919568_33

Guerrero, M., 2001. Secure ad hoc on-demand distance vector routing. ACM SIGMOBILE Mobile Comput. Commun. Rev., 6: 106-107. DOI: 10.1145/581291.581312

Guerrero-Zapata, M. and N. Asokan, 2002. Securing ad hoc routing protocols. Proceedings of the 1st ACM Workshop on Wireless Security, Sept. 28-28, ACM Press, Atlanta, GA, USA., pp: 1-10. DOI: 10.1145/570681.570682

Guo, Y. and M. Simon, 2010. Network forensics in MANET: Traffic analysis of source spoofed DoS attacks. Proceedings of the 4th International Conference on Network and System Security, (NSS), Sept. 1-3, IEEE Xplore Press, Melbourne, VIC., pp: 128-136. DOI: 10.1109/NSS.2010.45

Hamid, A., M.O. Rashid and C.S. Hong, 2006. Routing security in sensor network: HELLO flood attack and defense. Next-Generation Wireless Syst.

Lim, H. and C. Kim, 2001. Flooding in wireless ad hoc networks. Comput. Commun., 24: 353-363. DOI: 10.1016/S0140-3664(00)00233-4

Mulert, J.V., I. Welchn and W.K.G. Seah, 2012. Security threats and solutions in MANETs: A case study using AODV and SAODV. J. Network Comput. Appli., 35: 1249-1259. DOI: 10.1016/j.jnca.2012.01.019

Perkins, C. and E.M. Royer, 1999. Ad-hoc on-demand distance vector routing. Proceedings of the 2nd IEEE Workshop on Mobile Computing Systems and Applications, Feb. 25-26, IEEE Xplore Press, New Orleans, LA., pp: 3-12. DOI: 10.1109/MCSA.1999.749281

Silva, R.D., 2004. A security architecture for active networks. Proceedings of the 4th WSEAS International Conference on Applied Informatics and Communications Article, (WICAICA' 04).

Singh, V.P., S. Jain and J. Singhai, 2010. Hello Flood Attack and its Countermeasures in Wireless Sensor Networks. IJCSI Int. J. Comput. Sci. Issues, 7: 23-27.

Song, J.H., F. Hong and Y. Zhang, 2006. Effective filtering scheme against RREQ flooding attack in mobile ad hoc networks. Proceedings of the 7th International Conference on Parallel and Distributed Computing, Applications and Technologies, Dec. 4-7, IEEE Xplore Press, Taipei, pp: 497-502. DOI: 10.1109/PDCAT.2006.59

Theodorakopoulos, G. and J.S. Baras, 2006. On trust models and trust evaluation metrics for ad hoc networks. IEEE J. Selected Areas Commun., 24: 318-328. DOI: 10.1109/JSAC.2005.861390

Williams, B. and T. Camp, 2002. Comparison of broadcasting techniques for mobile ad hoc networks. Proceedings of the ACM International Symposium on Mobile Ad Hoc Networking and Computing, Jun. 09-11, ACM Press, Lausanne, Switzerland, pp: 194-205. DOI: 10.1145/513800.513825