ARUNAI PUBLICATIONS

Asian Journal of Applied Research

DOI: http://dx.doi.org/10.20468/ajar.2018.02.01

Research Article

Ad hoc On-demand Distance Vector Routing Protocol for Detection of Packet Dropping Attacks on Mobile *Ad Hoc* network using Enhanced Adaptive Acknowledgment

Abubucker Samsudeen Shaffi, S. Santhosh Baboo

Department of Computer Science, D. G. Vaishnav College, Arumbakkam, Chennai - 600 106, Tamil Nadu, India

Address for correspondence: Abubucker Samsudeen Shaffi, Department of Computer Science, D. G. Vaishnav College, Arumbakkam, Chennai - 600 106, Tamil Nadu, India
E-mail: shaabi75@rediffmail.com

ABSTRACT

Mobile *ad hoc* network (MANET) is interconnected through wireless links which are an arrangement of small portable devices; it can move freely based on the network of mobile nodes. Nodes in MANET can communicate with each other if and only if all the nodes are in the same range. This wide distribution of nodes makes MANET vulnerable to various attacks such as packet dropping attack is one of the possible attack. This is hard to detect and prevent these types of occurrences. In reactive routing protocol of *ad hoc* on demand distance vector finding the route on demand, when one of the nodes needs to send information to another node. This paper proposed the detection system with malicious attacks of enhanced adaptive acknowledgement (EAACK) which is specially designed for MANET. To prevent from selfish nodes, detection of misbehavior links and packet dropping attacks EAACK plays the significant role for securing MANETs.

Keywords: Packet dropping, *Ad hoc* on demand distance vector routing, Enhanced adaptive acknowledgment, Detection, Mobile *ad hoc* networks

Received: 02nd December 2017
Accepted: 20th December 2017
Published: 05th January 2018

INTRODUCTION

Mobile ad hoc network (MANET) has the properties such as wireless and mobility and also it is a collection of nodes.[1] MANET can independently move to other nodes s in any direction and change their links in network frequently which have self-configuring and dynamic network topology. It consists of nodes without a fixed infrastructure[2] and working supportively in *ad hoc* manner of self-configuring network. MANET is movable in a random manner where each node is free to move. The dual behavior of MANET is acts as both host and router, where the salient distinct feature of each node. Nodes of MANET include laptops and cell phones which have inadequate computation, energy resources, and communication.

Routing protocols

MANET consists of three types of routing protocols. These are categorized reactive, proactive, and hybrid routing protocol. *Ad hoc* on-demand distance vector (AODV) is purely on-demand routing protocol. It begins the route discovery process by spreading of route request (RREQ) message to its neighbor when a node of source wants to converse with another node containing the latter identified for that destination of the sequence number. Each of the node that backs to the source node and also generates an inverse route for the situation that forwards the RREQ.

Packet dropping attack occurred in MANET

The denial of service is the form of packet dropping attack, instead of forwarding them a node in the network will drop the packets. Figure 1 specifies the source represented with S will send the nodes to the destination D. We are specifying the route. The intermediate nodes are represented with {n1, n2, n3….. nk}. The auditor is capable of identifying the traffic patterns and also to detect the lost packets. The packet loss can be either of the link errors or the node failure.

This benevolent of attacks is very difficult to detect and prevent[3-5] due to number of different reasons when the node becomes compromised because it occurs. These can be dividing into several groups in terms of strategy which can be adopted by the malicious node to launching the attack. It is more vulnerable to security-based attacks due to their special features such as multi-hop routing, memory resources, inadequate battery, no

fixed infrastructure, and lack of centralized system.[6] Many of routing protocol developed for MANET but no other protocol is secure the networking efficiently.

- All the forwarded packets were purposely drop by the malicious node which going through it.
- The packets were selectively drop from originated or destined node in which the malicious node dislikes.
- This occurrence keeps the portion of packets by malicious node while the rest is usually communicated one packet in a certain time window or one packet out of N received packets.

To originating the packet dropping attack, the compromised node will convey the note by shortest path to a destination. By means of compromised node, transmission of all the packet will be directed and the node which is able to drop the packets.[5,7] The attack can be identified through the common networking tools, only if the malicious node attempts to drop all the packets. Hence, there is no packet transmission through the compromised node. However, it is very hard to detect the packet dropping attack, if the malicious router begins dropping packets on a specific Period of time or over every n packet, because some packet transmission still flows across the network. The prevention and detection of selfish nodes and packet dropping attack play a significant role in MANET.[4,5,7,8]

PACKET DROPPING IN AODV

The process between the source (S) and destination (D) of route discovery process under the routing protocol of AODV is shown in Figure 2 [10]. The source broadcasts a RREQ (Route Request) message with unique identifier to all its one hop neighbors. Each receiver rebroadcasts this message to its one hop neighbors until it reaches the destination.

Receiving the message at the destination which updates the source of the sequence number and sends message back route reply (RREP) to its neighbor which can be transmitted to the RREQ. There has the route to the destination of an intermediate node with the destination of order number which is equal to the one in RREQ to the source node can send back a RREP packet without transmitting to the destination.

To launching the packet dropping attack for a node at least one routing paths must be sophisticated in the network. This shown in Figure 2 C is denoted as a malicious node which is intending to packet drop from S to D. To discover a path from S to D, S first broadcasts RREQ packet to its neighbors. Each neighboring node continues to rebroadcast this message as explained earlier until it reaches D.

The C represents malicious node which disobeys the rule to claiming S which it has the direct path to D and sends the message RREP packet to S. As a result, S undertakes that the direct route to D which is through C and starts to send packets data through C to D which are, in turn, dropped.

MALICIOUS PACKET DROPPING

Malicious node is the initial step for initiation a packet drop attack which gets involved during the formation of routing. This is improved done by developing the vulnerabilities used in MANET with generally familiar routing protocols between nodes in a network which are proposed creating on the assumption of consistency. Once in the route, the malicious node can do anything including maliciously dropping packets. The malicious intermediate node of packet dropping is a detrimental situation which can lead to wrong information generation or suspension of communication between the source and destination. Figure 3 shows the subsequent designs of improved understanding in MANET used AODV routing protocols of malicious packet dropping scenarios.

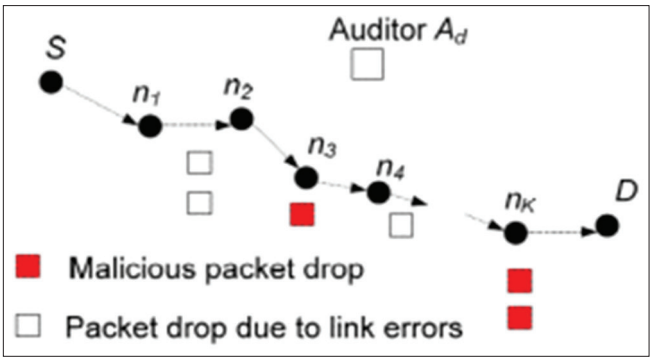

Figure 1: Packet dropping attack [13]

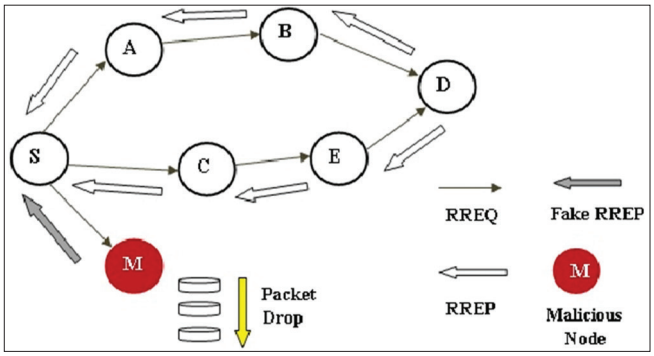

Figure 2: Packet Dropping Attack in AODV [10]

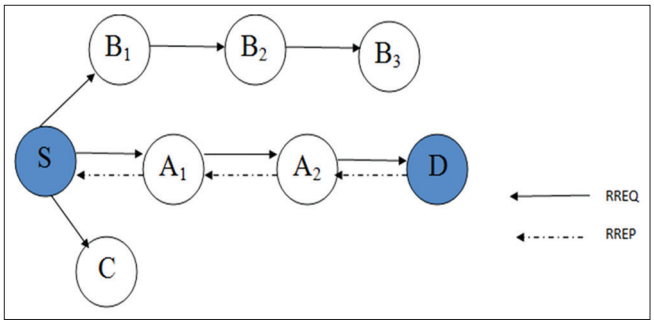

Figure 3: Route Discovery in AODV [12]

Data	ACK	S-ACK	MRA

Figure 4: Enhanced adaptive acknowledgment protocol in Manets [11]

SELFISH NODES DETECTION IN MANETS

In this section, EAACK approach is planned to covenant with malicious attacks. To prevent and detect the selfish nodes, finding of misbehavior links and packet dropping attacks, EAACK plays the significant role, which is mainly used for detecting routing misbehavior.

Enhanced adaptive acknowledgment scheme (EAACK)

EAACK used an acknowledgment based detection scheme enhanced AACK approach, Figure 4 shows contains 3 parts such as:

- ACK, secure
- ACK (S-ACK), and
- Misbehavior report authentication (MRA).

ACK is based on end-to-end acknowledgment scheme.[10]

In ACK mode, S be the source node will send an ACK packet of data to D which is destination node through the intermediate nodes. The endpoint node D will receive the acknowledge data packet effectively if all the in-between nodes are supportive. After acceptance, the ACK data packet, the end node D will send an ACK acknowledgment packet over the similar route. The packet transmission is successful from S to D, if S receives the ACK acknowledgment packet within a predefined period or else S node will switch over to S-ACK manner over sending out an S-ACK packet data. In the mode of S-ACK, the third node is necessary to direct an acknowledgment packet data of S-ACK to the initial node for every three successive nodes in the route. These three consecutive modes which are cooperatively work in a group in the network to detect the nodes of misbehaving. In TWOACK approach, the source node immediately trusts the misbehaving report, whereas in EAACK scheme, the source node will switch to MRA mode to conform the misbehaving report. In MRA mode, the source node will send MRA packet to the destination node through different paths for authentication. When the destination node receives the MRA packet through some route, then it will compare the MRA packet with its local knowledge base. If the MRA packet is already received through the same route then it will conclude that a node in that route has generated the misbehavior information is noticeable as malicious. Otherwise, the MRA packet is reliable and acknowledged.

Digital signature is used in this approach. All packets are essential to be digitally employed by its sender and proved by its receiver. This approach resolves false misbehavior, inadequate broadcast of power and receiver impact difficulties of watchdog approach. However, it will not detect partial dropping of packets by the intermediate malicious nodes.

CONCLUSION

In this paper, EAACK intrusion detection system is detect the misbehave report in the network. It is not possible in watchdog as well as in the two ACK schemes. Several drawbacks in the existing systems were overcome using this system. The EAACK system is very much secured and plays a significant role which is mainly used for detecting routing misbehavior. In future, it will compare with popular mechanisms. Security is the main issue in MANET, so partially it is satisfied by EAACK intrusion detection system.

REFERENCES

1. Akbani R, Korkmaz T, Raju GV. Mobile *ad-hoc* Network Security. In: Lecture Notes in Electrical Engineering. New York: Springer-Verlag; 2012.
2. Jayakumar G, Gopinath G. *ad-hoc* mobile wireless networks routing protocol-A review. J Comput Sci 2007;3:574-82.
3. Djahel S, Abdesselam FN, Zhang Z. Mitigating packet dropping problem in mobile ad-hoc networks: Proposals and challenges. IEEE Commun Surv Tutorials Fourth Quart 2011;13:658-72.
4. Hernandez E, Serrat MD. Improving selfish node detection in MANETs using a collaborative watchdog. IEEE Commun Lett 2012;16:642-5.
5. Kang N, Shakshuki E, Sheltami T. Detecting Misbehaving Nodes in MANETs. Paris, France: In Proc. 12th Int. Conf. ii WAS; 2010,
6. Goyal P, Batra S, Singh A. A literature review of security attack in mobile *ad-hoc* networks. Int J Comput Appl 2010;9:11-5.
7. Kang N, Shakshuki E, Sheltami T. Detecting Forged Acknowledgements in MANETs. Singapore: In Proc. IEEE 25th Int. Conf. AINA, Biopolis; 2011.
8. Nasser N, Chen Y. Enhanced intrusion detection systems for discovering malicious nodes in mobile *ad hoc* network. Scotland: In proc. IEEE Int. Conf. Commun., Glasgow; 2007.
9. Wu X, Yau DK. Mitigating Denial-Of-Service Attacks in by Incentive-Based Packet Filtering: A Game Theoretic Approach. In proc 3rd International Conference on Security and Privacy in Communications Networks; 2007.
10. Shakshuki E, Kang N, Sheltami T. EAACK-A Secure Intrusion-Detection System for MANETs. IEEE Trans Ind Electron 2013;60:1089.

Cite this article: Shaffi AS, Baboo SS. Ad hoc On-demand Distance Vector Routing Protocol for Detection of Packet Dropping Attacks on Mobile Ad Hoc network using Enhanced Adaptive Acknowledgement. Asian J Appl Res 2018;4(3):1-3.

Source of Support: Nil, **Conflict of Interest:** None declared.