International Journal of Computer Science
and Engineering (IJCSE)
ISSN(P): 2278-9960; ISSN(E): 2278-9979
Vol. 5, Issue 3, Apr - May 2016, 1-6
© IASET

International Academy of Science,
Engineering and Technology
IASET Connecting Researchers; Nurturing Innovations

PACKET DROPPING ATTACK DETECTION TECHNIQUES IN MANETS: A REVIEW

SAIRA AZIZ[1], ROHIT SETHI[2] & VARUN DOGRA[3]

[1]M. Tech Student, School of CSE and Engineering, Lovely Professional University, India

[2,3]Assistant Professor, School of CSE and Engineering, Lovely Professional University, India

ABSTRACT

Mobile ad hoc networks (MANET) are an autonomous system of mobile nodes connected by wireless links. Each node can act as a host (sender or receiver) or a router for forwarding the data packets in the network. Mobile ad hoc networks have several issues like routing, multicasting, quality of service, dynamic topology and energy constrained operation etc. An attacker can exploit the cooperative nature of mobile nodes and routing protocols to launch an attack. Security attack in MANETs are divided into two broad categories active attacks and passive attacks Packet dropping attack is an active attack in which attacker wants to drop the packets during the communication between sender and destination to decrease the throughput. In this paper, we present the review on packet dropping attack detection approaches with their pros and cons.

KEYWORDS: Confidant, Manet, Packet Dropping Attack, PathRater, Side Channel Monitoring, TWO-ACK, Watchdog

INTRODUCTION

Mobile Ad Hoc Network is a collection of mobile nodes which can communicate with each other through temporary wireless transmission links without the aid of an established infrastructure [7]. MANET is an appropriate solution in those areas where established infrastructure is damaged or impractical. Some of its applications are military services, rescue services in case of natural disaster like earthquake, distribution of information outside an office environment like in case of field work and offsite meeting etc. Following are the various unique characteristics of MANET and their impact on security:

- **Dynamic topology:** Nodes are mobile in nature, so topology changes constantly which leads to change in the routing information.
- **No administration:** There is no centralized management in MANET due to which detection of attacks and monitoring traffic will get difficult. It will also hinder the trust management for nodes.
- **Unreliability of wireless links between nodes:** MANETs are more vulnerable to security attacks as transmission takes place in open medium.
- **Multi-hop:** if sender and receiver are not in each other transmission range, then intermediate nodes can take part in the routing to relay the message in multi-hop scenario. This feature presents vulnerability because of the possible untrustworthy of intermediate nodes.
- **Amorphous:** The size and shape of the network is not known because of nodes mobility.
- **Computation and battery consideration:** Nodes are light weight terminals. For these nodes, a system design

criterion for optimization and energy conservation is most important, so security solution should consider it.

PACKET DROPPING ATTACK IN MANET

A packet may drop under following conditions:

- Selfishness of a node: Nodes behave selfishly and fail to forward the received packets in order to conserve their limited resources battery power [6].
- Validity of a node: A packet may drop because of network congestion or channel conditions (free path loss, interference, noise etc) or shortage of energy [12].
- Maliciousness of a node: A node may behave maliciously and drop the packets under attack by an intruder.

PACKET DROPPING ATTACK DETECTION TECHNIQUES

There are various packet dropping attack detection and prevention techniques to detect and isolate the malicious and selfish nodes from mobile ad hoc network. In this section, we illustrated some of the major detection approaches for packet dropping attack:

Watchdog and PathRater

Marti et al. [9] proposed Watchdog and PathRater method to detecting and mitigating routing misbehaviour. Every node should perform watchdog and pathrater in the network. According to this method, each node watch its one hop neighbour after sending the packet to confirm whether it forwards the packet or not On the basis of this monitoring, the pathrater can rate nodes. Nodes will exchange rating with every other nodes in the network. This helps the pathrater to choose the reliable links to forwards the data packets. Advantage of this method is that DSR with watchdog can detect misbehaviour nodes at the forwarded level not just the link level. Weakness of the Watchdog is ambiguous collision, false misbehaviour, receiver collision, insufficient transmission power, cooperated misbehaviour and partial dropping.

Confidant

Buchegger et al. [8] proposed a protocol called CONFIDANT (Cooperation of Nodes: Fairness in Dynamic Ad hoc Networks). It has four components: monitoring system, trust manager, reputation system and path manager. Each node monitors its neighbourhood nodes and observes routing protocol behaviour to detect misbehaviour. Trust manager deals with incoming and outing Alarm messages. Reputation system maintains the table for entries of each node and their rating. Path manager is used for path re-ranking and deletion or ignoring on the basis of the reputation of the nodes in the path. However, CONFIDANT depends on Watchdog mechanism, and therefore it also has many of its problems like false misbehaviour and collaborative attack.

Twoack

Balakrishnan et al. [2] proposed two acknowledgement based schemes TWOACK AND S-TWOACK They used acknowledgement packets called TwoAck packets, which are assigned a fixed route of two hops (or three nodes) in the direction opposite to that data packet. Ack in TCP are used for the purpose of flow control and reliable end-to-end communications where TwoAck is used to detect and isolate misbehaving nodes. The sender or router of a data packet should maintain the list of data packets Ids that have yet to receive a TwoAck acknowledgement packet from a node two hops away. This list is maintained by every node for each of its forwarding link that it is using. If a data packet ID stays on the list for longer than timeout then that misbehaviour link is suspected. When counter value reaches threshold for that particular link, a node declare it misbehaving link but in case of genuine route failures due to mobility or excessive traffic, node will generate RERR packet source.

In S-TWOACK, a node waits until a certain number of data packets arrived instead of a data packet is received. It reduces routing overhead but generates the problem of false alarms because genuine TwoAck packets lost is more noticeable.

Liu et al. proposed 2ACK scheme in [4]. This scheme is different from TWOACK in two ways. Firstly, In TWOACK , recipient need to send acknowledgment for every data packet where as in 2ACK, acknowledgment need to be sent for a fraction of message to reduce the routing overhead and congestion in the network caused in TWOACK. Secondly, it uses digital signatures to ensure the integrity of the acknowledgement packets. It has solved the problems of ambiguous collisions, receiver collisions, limited transmission power and limited overhearing range.

Aack

A. Al-Roubaiey proposed adaptive acknowledgement scheme in [1]. The AACK is combination of an Enhanced-TWOACK (E-TWOACK) scheme and an end-to end acknowledgment scheme. AACK has less routing overhead and works on node detection instead of link detection in TWOACK. Source node will receive acknowledgment from the recipient means all nodes in the route has forward and overhears the message are well behave nodes. When a malicious node is detected by other node, then it is that node responsibility to trigger the alarm to inform the other nodes including source node about the malicious node. It solves receiver collision and limited transmission power but suffer from partial dropping.

Side Channel Monitoring

Li et al. [13] proposed side channel monitoring (SCM) technique to detect packet drop attack in ad hoc networks SCM use two channels: primary channel and side channel. The set of nodes adjacent to the each node in the active route for communication will be selected as observer to monitor the message forwarding misbehaviour. Nodes of active route are part of primary channel and observer nodes are part of side channel. After detecting misbehaviour, the monitor nodes inform the source node by sending alarm message through both the channels. . SCM is able to detect the cooperative attacks and involves local communication only. But there is no encryption technique to secure the channels. Also, nodes performing partial dropping are undetectable.

COMPARISON OF VARIOUS DETECTION TECHNIQUES

Table 1: Comparison of various Detection Techniques and Their Weakness

Detection Technique	Contribution	Issues
Watchdog	Built on DSR protocol and gain the benefits of increased no of nodes while minimizing the effects of malicious nodes.	Watch dog fails in receiver collision, ambiguous collision, limited transmission power, partial dropping, false misbehavior and collaborative attacks.
pathrater	Uses link reliability data, kind of reputation system to rate the path and watchdog technique.	Cannot detect partial dropping and collaborative attacks.

TWOACK	Acknowledgment scheme added on DSR. It detects and isolates the misbehaving link.	Every packet should be acknowledged by the recipient that may lead to congestion in the path.
2ACK	Acknowledgement for only fraction of data sent plus authentication mechanism to check integrity.	Can’t find the misbehaving node as it only detect misbehaving link and eliminate it.
AACK	AACK solves the two problems i.e. Limited transmission power and receiver collision of watchdog technique by improving the TWOACK technique.	It may not work well on long paths because of the delay in end to end acknowledgements. Partial dropping
SCM	Involves local communication only. Also find collaborative attack	Can’t generate alarm message for partial dropping. No encryption technique to secure the channel

CONCLUSIONS

Security is an important factor in mobile ad hoc network. Mobile ad hoc networks are more vulnerable to security attacks including packet dropping attacks because of some issues like limited resources, unreliability of wireless links and intermediate nodes, no central administration and dynamic topology etc. We analyzed some of the malicious packet dropping techniques that detect and isolate the malicious nodes from the network. Although these techniques are capable of detecting and isolating the misbehaving nodes and link from the network but still there is every scope for fine tune alarm system and rating system.

REFERENCES

1. Al-Roubaiey, T. Sheltami, A. Mahmoud, E. Shakshuki, H. Mouftah, “AACK: Adaptive Acknowledgment Intrusion Detection for MANET with Node Detection Enhancement, 24th *IEEE International Conference on Advanced Information Networking and Applications*, 2010.

2. Balakrishnan, K.; Jing Deng; Varshney, V.K., "TWOACK: preventing selfishness in mobile ad hoc networks," *Wireless Communications and Networking Conference*, *IEEE* , vol.4, no., pp. 2137-2142 Vol. 4, 13-17 March 2005.

3. Jaydip Sen, M. Girish Chandra, P. Balamuralidhar, Harihara S.G., Harish Reddy “ A Distributed Protocol for Detection of Packet Dropping Attack in Mobile Ad Hoc Networks”, *Proceedings of the 2007 IEEE International Conference on Telecommunications and Malaysia International Conference on Communications*, 14-17 May 2007.

4. K. Liu, J. Deng, P. K. Varshney, and K. Balakrishnan, "An Acknowledgment-based Approach for the Detection of Routing Misbehavior in MANETs," *IEEE Transactions on Mobile Computing*, vol. 6, no. 5, pp. 536-550, May 2007.

5. Kajal S. Patel and Dr. J. S. Shah, “Detection and avoidance of malicious node in MANET”, IEEE *International Conference on Computer, Communication and Control* (IC4-2015).

6. Kennedy Edemacu1, Martin Euku2and Richard Ssekibuule, "Packet Drop Attack Detection Techniques in Wireless Ad Hoc Networks: A Review", *International Journal of Network Security & Its Applications (IJNSA*), Vol.6, No.5, September 2014.

7. Mohamad Y. Alsaadi, Yi Qian , "Performance Study of a Secure Routing Protocol in Wireless Mobile Ad Hoc Networks*" IEEE*, 2007.

8. S. Buchegger and J.-Y. L. Boudec, "Performance analysis of the CONFIDANT protocol (cooperation of nodes: Fairness in dynamic ad-hoc networks)," in *MOBIHOC'02*, 2002.

9. S. Marti, T. J. Giuli, K. Lai, and M. Baker, "Mitigating Routing Misbehavior in Mobile Ad-hoc Networks," *Proceedings of the 6th Annual International Conference on Mobile Computing and Networking*, PP. 255-265, August 2000.

10. T. Prasannavenkatesan, R. Raja and P. Ganeshkumar, "PDA-Misbehaving Node Detection & Prevention for MANETs" *International Conference on Communication and Signal Processing*, April 3-5, 2014.

11. Tao Shu and Marwan Krunz, "Privacy-Preserving and Truthful Detection of Packet Dropping Attacks in Wireless Ad Hoc Networks", *IEEE Transactions on Mobile Computing*, 2012.

12. Venkatesan Balakrishnan and Vijay Varadharajan, "Packet Drop Attack: A Serious Threat to Operational Mobile Ad Hoc Networks" *Proceedings of International Conference on Networks and Communication Systems* (NCS 2005), pp 89-95.

13. Xu Li, Rongxing Lu, Xiaohui Liang, and Xuemin (Sherman) Shen, "Side Channel Monitoring: Packet Drop Attack Detection in Wireless Ad Hoc Networks" *IEEE ICC 2011 proceedings*.