ISSN: 0975-8585

Research Journal of Pharmaceutical, Biological and Chemical Sciences

Potential threats caused by malicious nodes and various counter measures available in MANET: A Survey.

P Suganya*, and CH Pradeep Reddy.

School of Info.Technology and Engg. VIT University, Vellore, Tamil Nadu, India.

ABSTRACT

MANET is a continuously self-configuring, decentralized, infra structure less network of mobile nodes connected without wires. MANETs are characterized by dynamictopology change, high mobility and limited resources. Due to the wireless and infrastructure less nature of MANET, they are more vulnerable to various threats. The primary requirement in MANET is the cooperation of all the nodes in the network for the efficient communication. If there is a malicious node which is not cooperating in the network may lead to false route which is a serious security concern. Hence the misbehaving nodes need to be isolated from the network in order to enhance efficient routing. This paper reviews various approaches to detect and isolate malicious nodes in MANET.

Keywords: Network Attacks, Worm hole, Gray hole, Black hole, AODV, Game theory

**Corresponding author*

INTRODUCTION

In the recent years MANETs have been used in various applications such as military battlefield, commercial sector, PAN Etc. due to the specific characteristics such as infra structure less nature, decentralized administration, self-organizing and adaptive features. The nodes communicate with each other using various routing protocols and the data is transferred between the nodes. The data loss may occur due to the mobility of the nodes, network partition, limited bandwidth and less battery power. Some of the nodes in the network may be compromised to act as malicious nodes. These nodes may lead to false route which in turn may either partially forward or discard the data packets. The data loss that occurs due to the misbehaviour of the nodes should be addressed. Otherwise it leads to the disruption of the network. There are various approaches to solve this problem. But still they are vulnerable to various attacks [1] such as black hole attack, grayhole attack, worm hole attack and rushing attack.

Various attacks

Black hole attack: In this attack the misbehaviour nodes drops the packet which is to be forwarded to the next node thereby reducing the packet delivery ratio.

Grayhole attack: This attack is almost same as black hole but the malicious nodes behaves as normal nodes initially. Later it starts to drop the packets.

Worm hole attack: In this attack a link is created between two nodes and if any data pass through that link, the malicious nodes tend to disrupt the communication in the network.

Rushing attack: In this attack the malicious nodes immediately respond with the route reply packet for the route request packets ahead of all the other nodes. The route reply packet may contain the false route.

Countermeasures

Cooperative Bait Detection Scheme (CBDS)

In the network that uses Dynamic Source Routing (DSR) protocol, the collaborative black hole attack and grayhole attack can be detected and prevented using Cooperative Bait Detection Scheme (CBDS) [2].
DSR involves two phases:

- Route discovery
- Route maintenance

In the first phase the route request (RREQ) packet is broadcasted to all the nodes in the network. The intermediate node upon receiving the RREQ replies with the route reply (RREP) message if it has a valid route to the destination in its cache. Otherwise it forwards the packet to the adjacent node. Each node adds its address information in the RREQ packet before forwarding to other nodes. The RREQ packet received by the destination contains the address of all the intermediate nodes it traversed. The destination replies with the RREP message through that established route for further data transmission. The detection mechanisms can be broadly classified into two categories.

- Proactive
- Reactive

In Proactive mechanism, the nearby nodes are constantly monitored in order to detect the compromised nodes [3][4]. The Reactive mechanism [5] is triggered by the destination based on the packet delivery ratio.

The CBDS approach combines both the proactive and reactive mechanisms. In this scheme the address of the nearby node is used as the bait destination address to detect the address of the compromised node using reverse routing technique. The address of the detected node is added to the black hole list. The other nodes are also informed about the black hole node. The destination can also trigger this scheme it there is decrease in packet delivery ratio. The detection in CBDS approach is done in three steps.

- Initial bait
- initial reverse tracing
- shifted to reactive defence step

The CBDS approach outperforms in terms of packet delivery ratio with reduced routing overhead. This can be extended for other type of collaborative attacks.

Trust management system

The next approach is trust management system to identify the misbehaving node and to make them behave properly [6]. Trust is considered as an important security factor of a node in the network.. Trust is categorized in to two types. In the first type trust relationship is established based on the direct interactions [7]. In the second type [8] trust relationship is established based on the direct observation as well as the recommendation suggested by the other nodes in the network. The second type is considered to be most effective since the misbehaving nodes can be identified before starting interaction with that node to avoid some unwanted communication. The possible attacks in recommendation based trust systems are selective misbehaviour attack, bad mouthing attack, time dependent attack, ballot stuffing attack and location dependant attack.

The trust relationship is computed by observing the behaviour of each node. Trust values are calculated based on the Bayesian statistical approach. The node that is observing the behaviour of other node is called evaluating node. Trust relationship is established and the decision making on whether to forward or drop the packets is done using the rate of the evaluated nodes. The ratings may vary due to the genuine reason and also due to the behaviour of malicious nodes. This problem can be resolved in this approach using dynamic clustering technique to identify the trustworthiness of the nodes. The clustering is done based on the following criteria.

- Confidence value based on the number of interactions
- Deviation test to obtain the similar information of the evaluated nodes.
- Closeness among the nodes

This approach filters the false recommendations suggested by the malicious nodes and also outperforms in terms of network throughput and packet loss.

Enhanced Modified AODV

The next technique to prevent and detect the collaborative black hole attack is Enhanced Modified AODV [9]. In [10] Data Routing Information Table is used to identify the malicious nodes. Normal AODV is extended by adding two control packets such as Secure Reliable Route Discovery Request (SRRD_REQ) and Reply (SRRD_REP) and Threshold Value. During the path discovery process SRRD_REQ packets are sent by the source along with the SRRD_ID which is the destination sequence number of the destination node. The destination node alone can send the SSRD_REP message to the source. Two new fields such as Reliability List (RL) and Threshold Value (TV) are added to the routing table entry. The algorithm for EMAODV involves two phases.

In phase I the source node that is ready to transfer data checks whether there is any reliable route to the destination in its routing able before initiating the route discovery process. If yes starts transferring data otherwise stimulate the route discovery process by broadcasting the REQ packets. The intermediate node which receives the REQ packet send the reply if it has update in its routing table otherwise forward it to the neighbour node. The destination node that receives REQ packet replies with the REP message. During the reverse path discovery each node upon receiving the REP message updates its routing table and also adds one more entry as the IP address of the source.

In phase II SRRD packets are forwarded to all the nodes that replied with the REP message. Now each node that receives SRRD packet checks the routing table for reverse path entry. If yes SRR_ID is set from SRRD and forwards it to the neighbour node from where it received REP message earlier. When it reaches the destination it replies with the REP message. No intermediate node can send REP message now and therefore the secure path is established. The EMAODV outperforms normal AODV in terms of throughput with reduced routing overhead.

Game theory Model

Game Theory [11] is another approach. Game theory is a tool [12] that resolves the selfish behaviour issues. In this technique Bayesian signalling game is adopted to identify the normal and malicious nodes. Perfect Bayesian Equilibrium resolves the difficulties in false information. There are two categories in the game theory, Cooperative and Non Cooperative. Many Players cooperate with each other for the success of the game in cooperative mode and there will be conflict between two or more players. There are three factors which are to be considered in a game. They are set of players, strategies and payoffs. Strategy is the next move of each player and Payoff is the immediate incentive remedy provided forthe loss or success of a particular state in a game. The cooperation enhancement among the nodes and discrimination of selfish nodes can be done using Payment and payoff estimation schemes [12]. In this game theory model the sender and the receiver are the two players who are participating in the Bayesian signalling game. The message is chosen from the set and sent by the sender. The set of actions that can be chosen by the receiver are cooperating and decline. The strategy of each node can be determined by the estimated payoff and belief update methodology. The strategy of the node can be classified into pure, mixed and Perfect Bayesian Equilibrium (PBE). The action for the players is chosen and the uncertainty of the nodes that is the trust should be identified by considering the payoff calculation. The belief update is done using Bayes rule. Each node has to update the trustworthiness of other nodes. The probability of cooperation the neighbour node can be decided by the belief updates. This approach reduces the utility of misbehaviour node and increases the utility of normal node in terms of increased throughput, reduced routing overhead and reduced routing latency compared to the other approaches.

Comparative Analysis

Table 1: Comparative study

Performance Metrics	AODV	CBDS	Trust Management	EMAODV	Game Theory Model
Throughput	90	91	90	90	91.2
Routing Overhead	High	Less	Less	Less	Less

CONCLUSION

The presence of malicious nodes in a network causes several threats to the performance of network. We discussed the impact of malicious nodes over critical functionalities of network such as routing. In this paper we have reviewed various attacks that can be performed by the malicious nodes. The countermeasures for various threats have been reviewed which are available in the literature. We have performed a comparative study using various metrics such as throughput and routing overhead with various routing techniques.

REFERENCES

[1] Rashid HafeezKhokhar, MD AsriNgadi&Satria Mandala, "A Review of current routing attacks in Mobile Adhoc Networks", International Journal of Computer Science and Security, 01/2008, vol 2, issue (3) 27.

[2] Jian-Ming Chang, Po-Chun Tsou, Isaac Woungang, Han-Chieh Chao and Chin-Feng Lai, "Defending Against Collaborative Attacks by Malicious nodes in MANETs: A Cooperative Bait Detection Approach" in IEEE systems journal, VOL 9, No 1, March 2015.

[3] Baadache and A.Belmehdi, "Avoiding black hole and cooperative black hole attacks n wireless ad hoc networks " ,Intl .J. Coput. Sci. Inf. Security, vol 7 , no 1, 2010.

[4] S.Marti, T.J.GiuliK.Lai and M.Baker, "Mitigating routing misbehaviour in mobile ad hoc networks", in Proc 6th Annu. Intl. Conf. Mobicom, 2000, pp 255-265.

[5] W.Wang, B.Bhargava and M.Linderman, "Defending against collaborative packet drop attacks on MANETs", in Proc. 28th IEEE Int. Symp. Reliable Distrib Syst., New Delhi, India, sep 2009.

[6] Antesar M. Shabut, Keshav P. Dahal, Sanat Kumar Bista and Irfan U.Awan , "Recommendation Based Trust Model with an Effective Defence scheme for MANETs" , IEEE Transactions on Mobile Computing, vol 14, no 10, Oct 2015.

[7] A.A.Pirzada and C.Mcdonald, "Establishing trust in pure adhoc networks", in Proc 27th Australasian Conf Computer Science 2004, vol 26, pp47-54.

[8] S.Bucheggar and J.Y.LeBoudee, "Self-policing mobile adhoc networks by reputation systems, IEEE communication MAg, vol 43, no 7, pp 101-107, Jul 2005.

[9] Anuj Rana, Vinay Rana, Sandeep Gupta, "EMAODV: Technique to prevent collaborative attacks in MANETs" , 4th International Conf on Eco-friendly Computing and Communication Systems, 2015.

[10] S.Ramaswamy, H.Fu, M.Sreekantaradhya, J.Dixonandd K. Nygard, " Prevention of cooperative black hole attack in wireless Ad-hoc Networks", International Conference on Wireless Networks(ICWN), 2003, p 1-7.

[11] BalasubramanianParamasivan, MAria Johan Viju Prakash and MadasamyKaliappan, "Development of a secure routing protocol using game theory model in MANETs" , Journal of Communications and networks, vol 17, no 1, Feb 2015.

[12] F.Li and J.Wu, "Attack and Flee: Game theory based analysis on interactions among nodes in MANETs" , IEEE Trans Syst, ManCybern, vol 40, pp 612-622, 2010.