Study of Detecting Malicious Nodes in MANET and Fault tolerance: A Survey

T. PARAMESWARAN, Dr. C. PALANISAMY, T. JASMINE SONIA

Abstract:

Malicious nodes affect the Performance of mobile ad-hoc networks seriously. Wireless ad-hoc networks are rapidly gaining in a mode of communication specifically in mobile sectors; MANET is designed with wireless devices without existing infrastructure. Finally the networks are very easy to deploy and used in business and Personal applications. To Provide a more flexible mode of communication; wireless ad-hoc networks are more desirable. Multi hop route is used to communicate with each other in ad-hoc networks. In a MANET, if malicious nodes are present, they reduce network connectivity effectively and affect falsely to be co-operative; but they are dropping data that are meant to pass on. These may result in isolated nodes and reduced network performance. To detect malicious nodes on mobile ad-hoc networks; the various appropriate measures is discussed in this paper.

Index terms- Fault tolerance mechanism, MANETs, Malicious nodes, Multi- hop route,

I. INTRODUCTION

The decentralized type of Wireless network and this network does not rely on a Pre-existing infrastructure like routers in wired or access points in wireless networks. The collection of mobile nodes called ad-hoc networks forms a temporary network without any centralized administration[5]. For forwarding data packets from other nodes in the network, the mobile nodes not only operate as a host but also operates as a router. The node that participates in an ad-hoc routing protocol allows it to create multi hop paths to any other node through the network. The mobile nodes dynamically establish routing themselves to form own network while on the move and is also called as infrastructure less network. It refers to a mode of operation of IEEE 802.11. The main challenge is building a MANET that equipping each device to maintain the information required to route traffic.

II. ROUTING PROTOCOLS

In ad-hoc Wireless networks, the standard routing protocols such as Ad-hoc on demand distance vector routing protocol and Dynamic source Routing are primarily intended to create single route between source and destination. multipath routing is the routing technique of using multiple alternative paths through a network and it includes Fault tolerance, increased Bandwidth or improved security. To compensate the dynamic and unpredictable nature of ad-hoc networks, the multiple paths between source and destination pairs can be used [1]. In multipath routing protocol, the malicious nodes may become a vulnerable target to explore and launch many kinds of attacks such as black hole attack, warm hole attack, rushing attack, and Sybil attack. In multipath routing protocols, malicious nodes can conclude the part or the whole network on the basis of capturing routing information and very hard to ensure about the confidentiality of routing information because of the open media Network environment in which node can capture packets.

III. VARIOUS SECURITY ATTACKS IN MOBILE ADHOC NETWORKS

A. Modification

Modification is a type of attack when an authorized party tampers with an asset and it not only gains access. For example, modifying message fields or by forwarding routing message with false values. a malicious node can redirect the network traffic and conduct DOS attacks in this modification attack.

B. Impersonation

By masquerading as another node. i.e. spoofing. A malicious node can launch many attacks in a network and When there is no authentication of data packets in current ad-hoc network , malicious node is present. When a malicious node misrepresents its identity in the network (such as altering its IP or MAC address in outgoing packets) and alters the target of the network topology that a benign node can either present spoofing is occurred.

C. Attacks through Fabrication

The fabrication is an attack in which an authorized party not only gains the access but also inserts counterfeit objects into the system. Fabrication is used to refer the attacks performed by generating false routing messages in MANET.

D. Gray hole attack

The MANET in gray hole attack is discussed. In gray hole attack it has two phases, a malicious node exploits the AODV protocol in the first phase to advertise itself as having a valid route to a destination node, with the intention of intercepting packets, even though the route is spurious., the node drops the intercepted packets in the second phase with a certain probability. This attack is more difficult to detect than the black hole attack where the malicious node drops.

E. DoS attack

Denial of service attacks aim at the complete disruption of the routing function and therefore aims at the whole operation of the ad-hoc network. Specific instances of denial of service attack include the sleep deprivation torture and the routing table overflow. In a routing table overflow attack, it disrupt the establishment of legitimate nodes and the malicious node floods the network with bogus route creation packets in order to consume the resources of the participating node. By constantly keeping it engaged in routing decisions, the sleep deprivation torture aims at the consumption of batteries of a specific node.

F. Black Hole Attack

In a black hole attack, the attacker intercepts the packet without forwarding. By forging a route to the destination a black hole attacker disrupts route discovery [1]. The attacker fully modify the packet and produce fraudulent information, that causes the network traffic diverted. Let take G as a malicious node. The malicious node G receives a Route Request It sends a Route Reply suddenly, and then can be transmitted within the shortest path by itself. Black hole attack sometimes called as grey hole attack that attracts more traffic and disrupts existing routes.

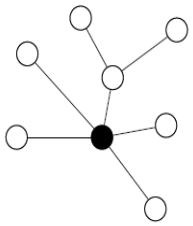


Fig. 1. Black hole attack

G. Warm hole Attack

In a Warm hole attack, the attackers can produce two or more black holes and connect them. That gives control over its packets and several parts of the MANET. This is one of the most powerful attack and it also known as tunneling attack.

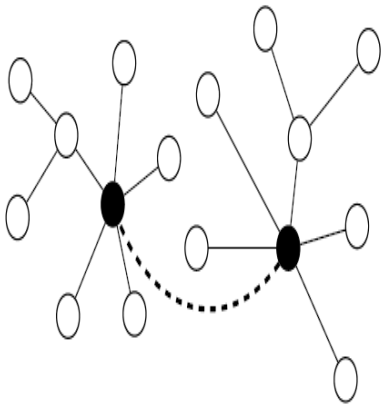


Fig. 2. Wormhole attack

H. Sybil Attack

In this attack, the attacker claim to have multiple identities. To generate this attack, first the attacker achieves the set of identity of legal nodes and impersonates all of them or some to participate in multiple route discoveries. By creating a more number of Pseudonymous identities, the attacker subverts the reputation system of a Peer to Peer network using them to gain a large influence. A vulnerability of a system to a Sybil attack depends on how the identities can be generated cheaply.

I. Rushing Attack In MANET

The one of the denial of service attacks called Rushing attack. In a Wireless communication system, before sending packet a normal mode waits for a random delay to avoid collision, and then the attacker forward data packets immediately.

K. *Blackmail Attack*

The Blackmail attack that use mechanisms which used for the recognition of malicious nodes and then broadcast the message to try to blacklist the offender. Adding other legitimate nodes to blacklists, attacker can blackmail the legitimate nodes. Thus the legitimate node can be avoided in those routes.

IV. DETECTION MECHANISM:

A. *Watch Dog Mechanism*:

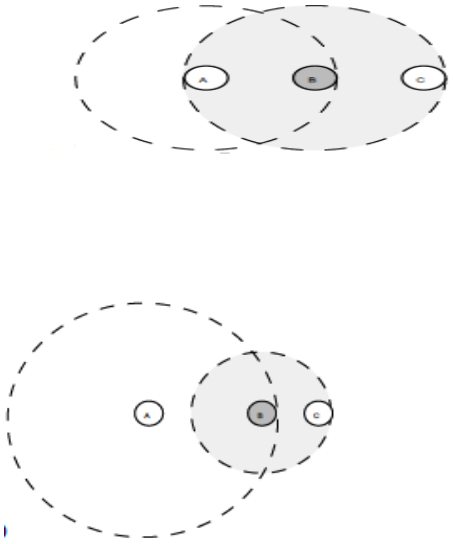


Fig. 3. a) A overhear B`s retransmission with equal ranges b) A cannot overhear B's retransmission [3]

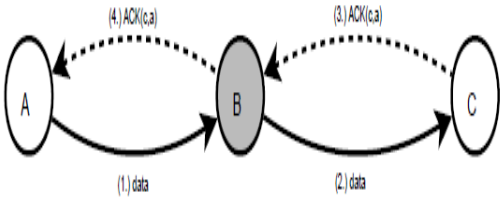
The Watch dog mechanism is very simple and has two disadvantages.1) It is error-prone: a collision causes both false negative detection and false positive detection. To have equal sending ranges, this model relies on all clients and using energy control this conflicts with modem WiFi-controllers.2) It does not speed this information, When a node recognizes its neighbor as nonparticipating, it is supposed to find only a new route. It is more useful to avoid selfish node and increase its throughput[3].

B. *Random Feedback*

The nodes can acknowledge forwarded packets across multiple hops by one can assume a working key management, among all nodes. The nodes A, B, C are part of a route. For every packet in C, A can include an encrypted nonce. For each received packet with the correct nonce C Can acknowledge. The intermediate node B cannot decrypt the nonce, thus it is suddenly recognized by a cheater or either has to forward the packet correctly [3]. This way of verifying every packet is very expensive. as shown in fig 4.

A suitable algorithm could present with often checks to check if a node is dependable and later use longer, random intervals between checks. This technique can easily be refined with A selectively requesting the acknowledgement. Then B has to forward all packets, if this request is encrypted as well because it cannot determine which ones include a request.

Fig. 4. Example of random feedback



architecture

C. *Distributed Reputation*

The distributed algorithms that led to the weakness of watch dog mechanism, in that every node periodically collecting ratings about its neighbours, and then distributing its ratings afterwards its calculating the reputation values from its own nodes as well as other nodes. In order to determine a distributed reputation, each and every step can be done in many different ways as well as there exist many different types of protocols.

D. *Mobile IDS*

All events in a MANET like nodes joining and leaving, route requests and replies, packets and data, amount of errors, and then attacks, observable patterns for various abnormalities that might be assumed. It is suggested that every node runs an intrusion detection agent that collects network events, analyses them, shares its data with other nodes' agents, and derives appropriate responses to detected attacks. First the system has to be trained with data from normal network operation. From then the collected data is analyzed by calculating the information-theoretic entropy and conditional entropy. If the conditional entropy from recent measurements differ from the previously trained values then an abnormality is detected and a reaction can be initiated Once a abnormality is detected locally, it should be passed to neighbouring nodes. By exchanging their data the mobile IDS agents should be able to detect abnormalities more accurately and to initiate not only local but also a global reaction.

E. TOHIP MECHANISM

In route messages, the Topology Hiding Multipath routing protocol does not contain link connectivity information. Thus by capturing route messages no node can deduce network topology. TOHIP can defend against attacks by using the combination of hop count and round-trip time as a routing metrics. Thus no warm hole attack can disrupt route discovery. By means of application layer TOHIP can excludes and detects the unreliable routes and it is topology hiding. Topology hiding can protect the network by hiding the network address and names for both the customer side and the core network side. The topology hiding also provides network protection for home gateway users or firewalls with private users. By using TOHIP mechanism, it does not allow any intermediate nodes to send reply messages thus it can resist black hole attack. In Worm hole attack the choosing of central positions is impossible and it is topology hiding thus it can resist worm hole attack. In Rushing attack, TOHIP uses hop count as a routing metric thus it can resist rushing attack. For resisting Sybil attack TOHIP mechanism is used and it is impossible to achieve the identity information of other nodes.

Table 1. Various Attack Detected By TOHIP

WATCH DOG	**RANDOM FEEDBACK**	**MOBILE IDS**	**DISTRIBUTED MECHANISM**	**TOHIP MECHANISM**
A misbehaving node dropping packets or manipulating packet is immediately identified and routes using this node can be avoided	If one assumes a working key management among all nodes, then nodes can acknowledge forwarded packets across multiple hops	The mobile IDS agents should be able to detect abnormalities more accurately and to initiate not only local but a global reaction	A distributed algorithms with every node periodically collecting ratings about its neighbours, and calculating reputation values from its own nodes	In TOHIP, the information is hidden so malicious node cannot deduce network topology. The reliable packet delivery can be achieved in TOHIP
Drawbacks: 1)Error Prone 2)does not speed this information	Drawbacks: 1)Very expensive 2)Need Various Algorithms	Drawbacks: The Normal Network operation is not supported in Mobile IDS	Drawbacks: The Protocols used are under criticism for the use of watchdog	Drawbacks: The faults that occur in MANET cannot be detected in TOHIP
Advantages: Dropping Packets is easily identified	Advantages :Among multiple hops the node can acknowledge forwarded packets	Advantages : The anormalities should be detected more accurately.	Advantages : The reputation values can be calculated from its own nodes.	Advantages: TOHIP can excludes and detects the unreliable routes and defend against attacks.

BLACK HOLE ATTACK	Does not allow intermediate nodes to send route reply messages.
WORMHOLE ATTACK	It is impossible for attackers to choose central positions and it is topology hiding.
RUSHING ATTACk	In Route Reply Phase, TOHIP uses hop count as a routing metric and thus resist attack
SYBIL ATTACK:	TOHIP is impossible to obtain the identity information of other nodes.

Table 2. comparision of various mechanisms.

IV. FAULT TOLERANCE

In Mobile ad-hoc Networks, Fault tolerance is one of the major design issue. To overcome the

Problem that occur in MANET, such as Node failures, link failure, transmission power, energy and location failures. The various detection algorithms are used to detect the failures with the help of FAULT DETECTION TECHNIQUE.

A. *Node Failures*

In Network, every node communicate with the nodes be located in the transmission range. For node communication, the node is not lie within the particular selection range and the middle node is used to pass the information to the hop. The node is not in the transmission range node failure will occur. To overcome the node failures in the network, Fault tolerant routing algorithm is used. In this algorithm; the networks is divided into grid and is based on geographical location information.[6] The Proposed FTRA Algorithm select alternate route from unused at hop in normal routing path. The route selection Performance is based on location information of its neighbhour grids.

B. Link And Network Failures

Due to fully or partially components in the network or any other natural disasters Link and network failures occur in MANET. Link failure will occur when the node can move away from the cluster. The model called trusted Fault tolerant is used in Location Aided Routing Protocol [7]. When the destination node moves away from the source location failures will occur. The Location Aided Routing Protocol concentrates on node congestion, high mobility and link faults. By using time out based method. MUTEX Algorithm is used to tolerate link and host failure.

C. Transmission Energy And Power Failures

The important issue in Mobile adhoc networks such as energy and power and Battery is most commonly used in the network and the power is commonly used for route selection, discovery, and repair the failures in the network.[8] The algorithm called fully distributed and Predictive control are used for optimizing transmission energy and power. A Fault tolerant Local spanning sub-graph algorithm is used in this technique and it is used to minimizes the transmission power.

D. *Other Approaches*

To achieve reliability and survivability in the fault detection and correction model, mobile ad-hoc networks and sensor networks use cross monitoring scheme. A Dynamic Protocol-DSDP called self-diagnosis protocol finds soft and hard faults in a fixed amount of time. For sharing the files the file replication technique is used in Mobile Ad-hoc network technique is used [4].

V. CONCLUSION

In this paper, various attacks in mobile ad-hoc networks is presented and it is detected with the help of various mechanism is discussed. In mobile ad-hoc networks the major design issue is fault-tolerance. To overcome the faults that occur in MANET various algorithm is presented and the faults in ad-hoc networks is detected by using this algorithm is discussed.

REFERENCES

[1] TOHIP: A topology-hiding multipath routing protocol in mobile ad hoc networks Yujun Zhang, Tan Yan, Jie Tian, Qi Hu, Guiling Wang, hong cheng Li Ad Hoc Networks 21 (2014) 109–122

[2] Malicious Node Detection System for Mobile Ad hoc Networks A. Rajaram *et al.* / (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 1 (2) , 2010, 77-85

[3] Detecting Selfish and Malicious Nodes in MANETs, Martin Schutte, Seminar: Sichereit In Selbstorganisierenden Netzen, Hpi/Universität Potsdam, Sommersemester, 2006

[4] Fault Tolerance in Mobile ad hoc Network: A. Dhanalakshmi D. Maheswari "A Survey International Journal of Advanced Research in Computer Science and Software Engineering"

[5] Jipeng Zhou and Chao Xia, "A Location-Based Fault-Tolerant Routing Algorithm for Mobile Ad Hoc Networks ", WRI International Conference on Communications and Mobile Computing, Volume 2 ,Page(s) 92 – 96,Jan 2009.,

[6] S. Chandrasekaran, S. Udhayakumar, U. Mohan Bharathy,and D. Jitendra Kumar Jain, " Trusted Fault Tolerant Model of MANET with Data Recovery ",4th IEEE International Conference on Intelligent Networks and Intelligent Systems(ICINIS), Page(s):21-24, 2011.

[7] O. Riganelli, R. Grosu, S.R. Das, C.R. Ramakrishna, and S.A. Smolka., " Power Optimization in Fault-Tolerant Mobile Ad Hoc Networks ",11th IEEE Conference on High Assurance Systems Engineering Symposium, Page(s): 362 - 370 ,Dec 2008.

[8] R.K. Sahu, R.Saha.R and N.S. Chaudhari, "Fault Tolerant Reliable Multipath Routing Protocol for Ad Hoc Network ", Fourth International Conference on Computational Intelligence and Communication Networks , Page(s) 117-121, Nov 2012.

[9] Giuseppe Anastasi, Alberto Bartoli and Flaminia L. Luccio ," Fault-Tolerant Support for Reliable Multicast in Mobile Wireless Systems: Design and Evaluation", Wireless Networks , Volume 10, Issue 3, pp 259-269, May 2004.

[10] Md. Ehtesamul Haque and Ashikur Rahman , "Fault Tolerant Interference-Aware Topology Control for Ad Hoc Wireless Networks", Ad-hoc, Mobile, and Wireless Networks ,Lecture Notes in Computer Science Volume 68, pp 100-116,2011.

[11] L. Demoracski,"Fault-tolerant beacon vector routing for mobile ad hoc networks ", 19th IEEE International Parallel and Distributed Processing Symposium, April 2005.

[12] Sheng Xu , S.Papavassiliou and L. Zakrevski," Fault-tolerant cluster-based routing approach in wireless mobile ad hoc networks", IEEE VTS 54th Conference on Vehicular Technology, Volume: 4 ,Page(s): 2613 – 2617, 2001.

[13] Yuan Xue and K. Nahrstedt, "Fault tolerant routing in mobile ad hoc networks", IEEE Conference on Wireless Communications and Networking, 2003, Volume: 2 ,Page(s): 1174 – 1179, March 2003.

Parameswaran T has received his B.E degree in Electronics and Communication Engineering from Vellalar College of Engineering and Technology, Erode, and M.E degree in Software Engineering from College of Engineering Guindy, Anna University Chennai in 2005 and 2008 respectively. He is currently pursuing his Ph.D. from Anna University, Regional Centre Coimbatore. He is currently working as Assistant Professor in the Department of Computer Science and Engineering, Regional Centre, Anna University, Coimbatore, India. He has published more than 10 research papers in various journals and conferences. He has organized 3 national level workshops.

Dr. C. Palanisamy has received his B.E degree in Electronics and Communication Engineering from University of Madras, Chennai and M.E degree (Gold Medalist) in Communication Systems from Thiagarajar College of Engineering, Madurai, Madurai Kamaraj University in 1998 and 2000 respectively. He has received his Ph.D from the faculty of Information and Communication Engineering, Anna University, Chennai in 2009. He has more than 13 years of academic and research experience and currently he holds the post of Professor and Head of the Department of Information Technology, Bannari Amman Institute of technology, Sathyamangalam and Tamilnadu, India. He has published more than 30 research papers in various.

Jasmine Sonia T has completed her B.E degree in Electronics and Communication Engineering from Jayaraj Annapackiam CSI Engineering College, Nazareth in 2013, and currently she is a PG scholar at Anna University Regional Centre, Coimbatore with a specialization of Network Engineering.

