VOL. 10, NO. 5, MARCH 2015 ISSN 1819-6608
ARPN Journal of Engineering and Applied Sciences


www.arpnjournals.com

AN INSIGHT ON REPUTATION BASED INCENTIVE SCHEME AND THROUGHPUT FEEDBACK ROUTING IN MANET'S

Christy Jackson[1], V. Vijayakumar[1], Subramaniyaswamy V.[2] and Anusooya G.[1]
[1]SCSE, VIT University Chennai, India
[2]School of Computing, SASTRA University, Thanjavur, India

ABSTRACT

A Dynamic wireless network which is composed without any actual infrastructure is a mobile ad-hoc network (MANET). Every potential node in the network deports as a router. These mobile networks are much more vulnerable than wired networks because of their restricted physical security, power constraints, network topology which keeps altering dynamically, and due to improper centralized administration. This paper portrays few attacks on each of OSI's network layer. It also confines some of the attacks faced by MANET. These attacks include packet drop, flooding, black hole, link spoofing, and wormhole. The intention of this paper is to survey the attacks on mobile ad-hoc networks and routing protocols.

Keywords: MANET, RBIS, TUF, DoS

1. INTRODUCTION

Mobile ad hoc networks (MANETs) represent complex distributed systems that comprise wireless mobile nodes. These nodes can freely and dynamically self-organize into arbitrary and temporary, ''ad-hoc'' network topologies, allowing people and devices to seamlessly internetwork in areas with no pre-existing communication infrastructure [11] e.g., disaster recovery environments. Recently, the introduction of new technologies such as the Bluetooth, IEEE 802.11 and HyperLAN are helping enable eventual commercial MANET deployments outside the military domain [3]. These recent evolutions have been generating a renewed and growing interest in the research and development of MANET

Some of the salient features of MANET would be it is self-operated without any infrastructure, Light weight terminal, multi hop routing, Distributed operation, Ease and speed of deployment [2]. Since these features are prone to attacks MANET experiences few security issues. Absence of infrastructure, limited physical security, restricted power supply, lack of centralized monitoring are few security issues which are to be looked upon while designing a mobile ad-hoc network [7]. MANET like any other networks focuses on achieving the basic security goals which are Availability, Authenticity, Integrity, Authorization, Confidentiality, Scalability, Non repudiation [2].

This paper attempts to provide a comprehensive overview of this dynamic field. It first explains the important role that mobile ad hoc networks play in the evolution of future wireless technologies. It goes on to explain some of the attacks that are faced by MANET. Finally routing protocols which are used to address the attacks are discussed and recommendations are provided.

Here introduce the paper, and put a nomenclature if necessary, in a box with the same font size as the rest of the paper. The paragraphs continue from here and are only separated by headings, subheadings, images and formulae. The section headings are arranged by numbers, bold and 10 pt. Here follows further instructions for authors.

2. SURVEY

Malicious and selfish nodes are the ones which construct the attacks. The attacks are usually caused in physical, data link, network, and application layer. Routing protocols commonly exhibited to two types of attacks active and passive attacks. Nodes that perform attacks with the intention to damage other nodes by stimulating a network breakdown are called as active attacks. Nodes which perform attacks with the aim of saving battery performance and life for their own communications are called passive attacks. These nodes can easily put down network performance and eventually partition the network [12].

2.1 Attacks on MANET based on each layer

2.1.1 Physical layer

Eavesdropping is a special kind of attack that could be found in MANET. It tries to capture confidential information such as location, private or public key, passwords that should be kept in secret. The next attack on the physical layer would be Interference and Jamming. The attacker sends signals with the same frequency and same intervals of time as the sender and receiver. This causes errors due to pulses and random noise during communication [7].

2.1.2 Data link layer

Denial of service is one of the notable attacks in the data link layer. In this attack malicious node floods the network with irrelevant data to use up the network bandwidth or resources of a specific node. This could be avoided with networks with infrastructure by discovering the neighbour node. Since mobile adhoc networks are infrastructure less it could cost more to find out the malicious node [7]. Spoofing is another attack faced when a malicious node misinterprets its identity and alters its destination network topology by changing their MAC or IP address [7].

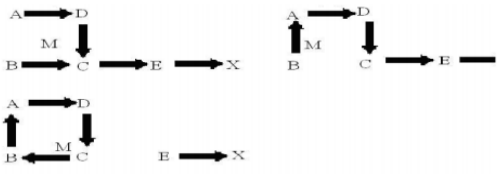

Figure-1. A sequence of events forming loops by spoofing packets.

2.1.3 Network layer

A malicious node publicizes as having a valid route to the destination. The attacker then consumes the node without forwarding and can alter data causing the network traffic to be diverted and dropped. Tunneling attack is also called as wormhole attack. The attacker gets the packet at one end and tunnels it to another point in the network. The malicious node is linked through a private network connection which is not visible at higher levels and hence it's called as tunneling attack.

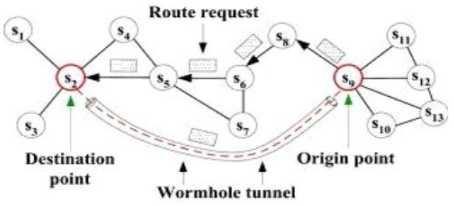

Figure-2. Wormhole attack.

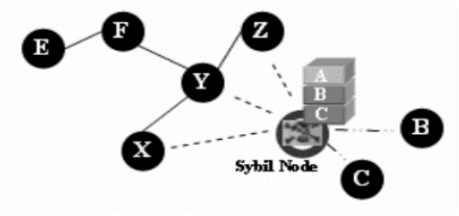

Figure-3. Sybil attack

Sybil node is another type of attack in which the malicious node not only impersonates they could put on the identity of few other nodes. By doing it undermines the redundancy of many routing protocols [7]. It attempts to degrade the integrity of data, security and resource utilization. Essentially any peer-to-peer network is vulnerable to Sybil attack

2.1.4 Transport layer

This layer is affected by an attack called as session hijacking. Most authentication processes are carried out only when a session starts which forms the point of entry for attackers. The malicious node tries to pretend as an authentication node and hijack the session [7].

2.1.5 Application layer

An attacker develops attacks which attack both operating system and user applications. This causes the computer system as well as the network to be damaged. Virus, worms, spyware, and Trojan horse are few common techniques used by attackers [7]. Therefore it is clearly evident that mobile ad hoc networks are vulnerable to these attacks and still a lot of other attacks as well. Thus in order to decrease the vulnerability there are lot of routing protocols designed to increase the network security. This paper deals with routing techniques which solves various Denial of service (DoS) attacks.

3. TECHNOLOGY

Denial of service is an attack which wipes out network capacity or bandwidth from performing its required function [5]. This prevents the authorized users to access their resources. They place threats to more prominent websites such as Amazon and eBay. It changes the routing algorithm or system configuration and attacks the network or the application. Unlike traditional networks MANET's are vulnerable to this type of attack. This is because in a mobile network the resources are confined and hence each node tries to be greedy in resource utilization. Battery power is another critical resource for mobile nodes. If the battery power has been used up due to malicious attacks such as the sleep deprivation attack, the victim will not be able to provide network services [4].

Few prevention detection techniques such as the cryptograph and authentication can provide better security to mobile networks. Nevertheless these protocols cause latency or overhead or can't prevent attacks by the malicious internal node. Most researches on MANET these days are concerning secure routing protocols. In this paper two different algorithms to address the denial of service attack are discussed. Throughput algorithm and Reputation based incentive scheme will be covered in this writing.

3.1 Reputation based on incentive scheme

Like other networks, the security requirements in ad hoc networks include services such as availability, authentication, non-repudiation, confidentiality, integrity, and access control. To defend a DoS attack it is necessary to both detect and prevent it. Most of the MANET routing protocols address either detecting or preventing, it is essential that both aspects are to be dealt for a successful MANET routing protocol [2]. Reputation based incentive scheme applies a combination of detection and prevention measures.

When an attacker is mobile, mechanisms such as trace back can be effective in determining the attack path or attack generating domain, but inefficient in identifying the attacking host as explained in [2]. Introducing some penalty to nodes which do not cooperate and committing incentives to nodes which cooperate improves security and performance in MANETs. A particular node which acts indifferent from its reputation and acts maliciously could be barred from the network. If they do not cooperate then

eventually it could be eliminated. In building reputation for new incoming node, the age of a node is taken into consideration for distinguishing it from the other nodes.

3.1.1 Proposed mechanism

It involves Cluster formation, reputation database construction, maintenance, and information exchange. Local reputation ratings can be incurred from neighbours or cluster heads. Attempts will be made to provoke nodes and monitor its behaviour. Nodes which do not behave are identified and are isolated in order to prevent from Dos attack [2].

3.1.2 Clustering architecture

A node is entitled to be a cluster head (CH) only if it has the required resources, in terms of battery power and lower relative mobility. Localized topology algorithm is used within a cluster whereas a distributed topology is used among the clusters. Each node in a cluster knows its neighbour by communicating with each other through messages. The cluster head node (CH) is employed to manage the network. Each node shares a common resource and is a member of a community. In a community a node with good reputation gains points whereas a node bad reputation will finally be eliminated from the network [2].

3.1.3 Reputation management

The main concern of reputation management is that how and where to store the data; it is divided in to four modules as shown in the diagram below.

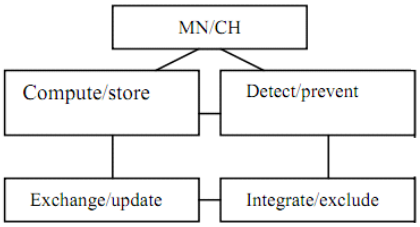

Figure-4. Data structure for reputation management.

Mobile nodes and the cluster head compute and exchange reputation ratings. It is necessary to integrate the local reputation data without a centralized storage and management facility as it is a mobile network. The possible options are to store the reputation of a few nodes in a particular node or the whole network. This algorithm uses a strategy in which all the reputation data of the nodes are stored in a cluster. This provides less overhead and better scope than the neighbour only strategy. A combination of peer-to-peer and banking on the cluster head for information exchange are two strategies that are adopted [2].

3.1.4 Dealing with misbehaving nodes

For management purposes each node periodically performs a set of iterative processes. Reputation ratings are worked out and on its own and second hand information from neighbour nodes and Cluster head are used to monitor the behaviour and classify it. Marks the node as selfish node and broadcasts the new reputation to all the other nodes and CH. Periodically reviews the reputation rating. Misbehaving nodes are first warned and later eliminated from the network. In case if they cooperate the packets are not forwarded till the reputation rating reaches a benchmark assigned [2].

3.2 Throughput feedback routing (TUF)

TUF is a multi-layer technique that detects attacks in transport layer and reacts to attacks in the network layer. It basically monitors the good throughput (good put) at the transport layer because most route disruption attacks such as the protocol compliant attacks degrade the good put of the transport layer [6]. TUF is capable of putting out protocol compliant attacks, few insider attacks such as the grey-hole attack, rushing, black hole and wormhole attacks.

3.2.1 Overview of the architecture

TCP being the most widely used transport layer protocol and is the target for all jelly fish attack (JF) is the principal focus of this routing technique. TUF is composed of two modules, Throughput monitoring (TM) and Route Rebuilding (RR). TM briefs the abnormalities in the route and it invokes the RR module which employs the least-alike re-routing algorithm (LARR) to work up a new route for the packets. The RR module is invoked when the malicious or abnormal node reaches a threshold and an alarm is evoked to trigger the RR module [6].

It is justified that this strategy is adopted by observing that most attacks of DoS lowers the TCP value of the ad hoc network and is possible to Figure out the possible good put value of a given ad hoc network. Consequently by the above two observation it is possible to find out an abnormal event by the significant gap between the estimated and the observed good put [6]. The added advantage of adopting this technique is that not only attacks but non attacks can also be addressed. There remains a gap even if there appears to be a non-attack (Routing failures due to wireless link connection or node mobility) and causes a drop in the good put. Fortunately TUF builds a new look alike route to maintain the good put irrelevant of the deterioration caused by an attack or a non-attack

3.2.2 Throughput monitoring (TM)

TM monitors route by periodically noticing the good put of which can be done by observing the 32 bit acknowledgement field number of the TCP header. This time is taken as‘t’ sec. Gth (bytes/sec) is denoted as the estimated threshold of acceptable throughput. If the observed time‘t’ is less than that of Gth then it signifies that there is a trouble in the route and raises the alarm. The Round Trip Time (RTT) between the source and

destination node ids employed to determine the value of't'. The average TCP throughput 'T' is determined with the following equation shown below

$$T = \frac{1}{RTT\sqrt{\frac{28}{3}p} + T_0 \min\left\{1, 3\sqrt{\frac{38}{8}p}\right\} p\left(1+32p^2\right)}$$

Where T0=2RTT is the timeout, B denotes the TCP maximum segment size (bytes), and p denotes the packet loss ratio. The packet loss ratio p can be found since RTT and B are known with the help of Route Request messages. Then the value of Gth set using the following equation.

$G_{th}=T.\ r_a$

Where ra is a co-efficient introduced to reduce the number of false positives [6].

3.2.3 Route rebuilding (RR)

The principal purpose of RR is to build a new route once the TM module invokes a new route request. The least alike re-routing (LARR) algorithm is intended to do this. The sender selects a new route from the cache with smallest likeness degree. If there are multiple numbers of routes that match the criteria, the route with the least number of nodes will be selected. Still if there remain two or more routes then the route with fewer indexes is chosen [6]. Thus by following methodology both attacks and non-attacks are encountered by throughput feedback routing.

4. ANALYSIS

In both TUF and Reputation based Incentive scheme there are few assumptions made in order to carry out the processes. These assumptions made lower the effectiveness of the technique because they signify that the algorithm would not function if these criteria are met.

4.1 Assumptions in reputation based incentive scheme

Each mobile node and cluster head in the network has a Unique ID. Each node could join or leave the network anytime. Reputation information exchanged between the nodes are assumed to be correct and no collusion between the nodes. Initially all nodes have the same storage capacity and equal computational though few nodes may have more resources during communication processes

4.1.1 Drawbacks due to the assumption

Some of the drawbacks when considering these assumptions are that any node can join or leave freely which could cause malicious node to enter with a counterfeit reputation and get mingled with the network. The nodes which enter and leave should be filtered to avoid this. The reputation information exchanged is considered to be correct always which is not possible at all situations.

4.1.2 Results of simulation

Experiment was conducted to find how long it takes to detect misbehaving nodes using the neighbor and cluster level reputation ratings. As seen in Figure-7 the detection rates increase from 80% to 99% for neighbors and from 76% to 97% with neighbor reputation information [2].

4.2 Assumptions in throughput feedback scheme

All links in the network to be bidirectional. It can address only network layer disruption attacks and does not cater to the attacks in the other layers. The next assumption is that in a communication process the source and destination are trustworthy and the intermediate nodes are not. It is also assumed that all packets used for controlling are authenticated using some security measures and does not deal with outsider attacks.

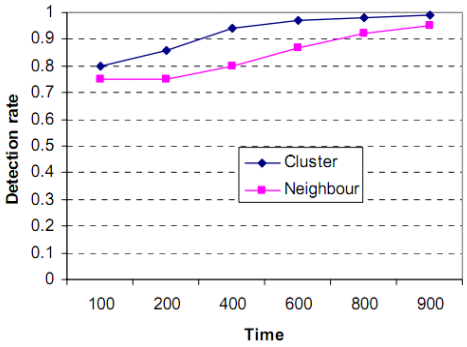

Figure-5. Delivery ratio as a function of misbehaving nodes.

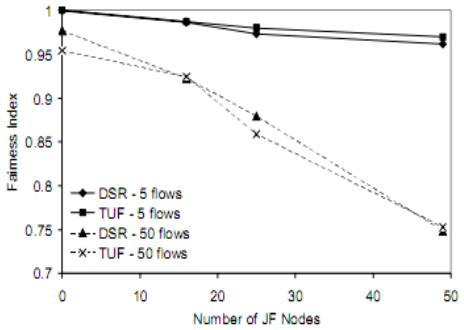

Figure-6. System fairness.

4.2.1 Drawbacks due to the assumptions

The assumptions made decrease the potency of the algorithm. Attacks are most prevalent in transport layer which is not been covered. If a source or a destination node becomes malicious the algorithm cannot detect the node.

4.2.2 Results of simulation

Figure-6 shows the result of an experiment done do check the system fairness. An index close to 1 is suitable as it signifies that the network bandwidth is shared

equally among all the nodes. The Figure also indicates that TUF does not affect system fairness, which implies that the increased throughput in TUF is relatively equal for every flow; no matter how many hops a flow has [6].

5. CONCLUSIONS

This paper addresses the attacks and routing protocols for mobile ad-hoc networks. The paper discloses various attacks that happen in each network layer. It goes on to address the Denial of Service attack and two routing protocols which reference various forms of DoS attacks. Key features of reputation based Incentive Scheme and Throughput feedback mechanism are discussed. Critical analyses of the two routing protocols are covered in this paper. TUF and Reputation based incentive algorithm could be more effective if it could reduce the assumptions made and taking those scenarios into consideration.

REFERENCES

[1] V. Balakrishnan, and V. Varadharajan. 2009. Packet Drop Attack: A Serious Threat to Operational Mobile Ad -Hoc Networks. Information and Networked System Security Research, vol. 1, pp. 12-16, February.

[2] R. Chen, M. Snow, J. M Park, M. T Refaei, and M. Eltoweissy. 2004. Defense against Routing Disruption Attacks in Mobile Ad Hoc Networks. Virginia Polytechnic Institute and State University, Virginia, ARIAS Tech. Rep, 90-96.

[3] M. Denko. 2005. Detection and Prevention of Denial of Service (DoS) Attacks in Mobile Ad Hoc Networks using Reputation-Based Incentive Scheme. M. Eng. thesis, University of Guelph, Guelph, Ontario, Canada, February.

[4] Y.H. Hu, A. Perrig, and D.B. Johnson. 2003. Rushing Attacks and Defense in Wireless Ad Hoc Network Routing Protocols. Computer and Communications Security, vol. 3, pp. 22-25, September.

[5] Y.H. Hu, A. Perrig, and D.B. Johnson. 2005. "Ariadne: A Secure On-Demand Routing Protocol for Ad Hoc Networks," Wireless Networks, vol. 11, pp. 21-38, December.

[6] Mehfuz, S.; Ali, I.; Thomas, M.S. 2008. "Ad Hoc Based Secure Architecture for Survivable and Reliable Substation Automation System," Power System Technology and IEEE Power India Conference, 2008. Powercon 2008. Joint International Conference on , vol., no., pp.1,6, 12-15 October. Doi: 10.1109/ICPST.2008.4745222

[7] M. Monika, M. Kumar, and R. Rishi. 2010. Security Aspects in Mobile Ad Hoc Network (MANETs): Technical Review. International Journal of Computer Applications, Vol. 12, pp. 37-43, November.

[8] Z. Slimane, A. Abdelmalek, M. Fahem, and A.T Ahmed. 2011. "Secure and Robust IPV6 Auto-Configuration Protocol for Mobile Ad-hoc Networks under Strong Adversarial model," International Journal of Computer Networks & Communications, vol. 2, pp. 208-227, July.

[9] Talwar, B., Venkataram, P., & Patnaik, L. M. 2007. A Method for Resource and Service Discovery in MANETs. Wireless Personal Communications, 41, 301-323.

[10] N. Vimala, and R. Balasubramanium. 2010. Distributed Key Management Scheme for Mobile Ad-Hoc Network-A Survey. Global Journal of Computer Science and Technology, vol. 10, pp. 7-11, April.

[11] M. Yadav, V. Rishiwal, and K.V. Arya. 2009. Routing in Wireless Adhoc Networks: A New Horizon. Journal of Computing, vol. 1, pp. 204-208, December.

[12] P. Yi, Z. Dai, S. Zhang, and Y. Zhong. 2003. A New Routing Attack in Mobile Ad-Hoc Networks. International Journal of Information Technology, vol. 11 no. 2, pp. 83-94, September.