International Journal of Engineering Research and General Science Volume 3, Issue 6, November-December, 2015
ISSN 2091-2730

Survey Paper For Detection Of Malicious Nodes In Routing Of Mobile Ad-Hoc Network

Bhavik Panchal (M.E Wireless And Mobile Computing)

GTU PG School Ahmedabad, bhavik_panchal17@yahoo.com and +919429457971

Abstract — To find method of detecting selfish and misbehaving node for providing better security in routing of adhoc network. First of all generate the adhoc network. In Adhoc network nodes are mobile so the network topology may change rapidly and unpredictably over time. The network is decentralized, where all network activity including discovering the topology and delivering routing messages is executed by the nodes themselves, so one or more of them may misbehave and disturb the network. The misbehavior or attack can be of many types.

In the network the node can work in two ways by exhibiting selfishness or misbehaviour and cause disturb once in the network by using different type of attack. To identify or detecting malicious or selfish node Intrusion Detection System (IDS) system is developed. It has different architecture for to detect malicious or selfish node. One is Stand Alone architecture and other is Distributed and co-operative architecture.

I will use Watch-Dog mechanism to detect selfish and misbehaving node that agree to forward packet but fails to do so. Path-rater is mechanism used for removing path from cache that contain malicious or selfish node.

Keywords— Ad-Hoc Network ,Watch-Dog , Intrusion Detection System (IDS),Security , Distributed , Stand Alone Architecture , Pathrater.

INTRODUCTION

During the last few years we have all witnessed a continuously increasing growth in the deployment of wireless and mobile communication networks. Mobile ad hoc networks consist of nodes that are able to communicate through the use of wireless mediums and form dynamic topologies. The basic characteristic of these networks is the complete lack of any kind of infrastructure, and therefore the absence of dedicated nodes that provide network management operations like the traditional routers in fixed networks. In order to maintain connectivity in a mobile ad hoc network all participating nodes have to perform routing of network traffic. The cooperation of nodes cannot be enforced by a centralized administration authority since one does not exist. Therefore, a network layer protocol designed for such self-organized networks must enforce connectivity and security requirements in order to guarantee the undisrupted operation of the higher layer protocols.

Security is an essential service for wired and wireless network communications. The success of mobile ad hoc networks (MANET) strongly depends on peoples confidence in its security. However, the characteristics of MANET pose both challenges and opportunities in achieving security goals, such as confidentiality, authentication, integrity, availability, and non-repudiation. We

provide a survey on attacks and countermeasures in MANET in this paper. The countermeasures are features or functions that reduce or eliminate security vulnerabilities and attacks. First, we give an overview of attacks according to the protocols stacks, and to security attributes and mechanisms.

Literature Review

S. Martiet [1]. provides the information of DSR Routing algorithm. The paper also describe two techniques that improve throughput in an adhoc network in the presence of nodes that agree to forward packet but fails to do so. To mitigating this problem we propose categorizing the nodes based upon their dynamically measured behavior. We use watchdog that identifies misbehavior node and pathrater that helps routing protocols avoid these misbehavior of nodes. Through simulation we evaluate watchdog and pathrater using packet throughput, percentage of overhead(routing) transmission and the accuracy of misbehaving node detection.

Network Security

A security protocol for ad hoc wireless networks should satisfy the following requirements. The requirements listed below should in fact be met by security protocols for other types of networks also.

Confidentiality: The data sent by the sender (source node) must be comprehensible only to the intended receiver (destination node). Though an intruder might get hold of the data being sent, he/she must not be able to derive any useful information out of the data. One of the popular techniques used for ensuring confidentiality is data encryption.

Integrity: The data sent by the source node should reach the destination node as it was sent: unaltered. In other words, it should not be possible for any malicious node in the network to tamper with the data during transmission.

Availability: The network should remain operational all the time. It must be robust enough to tolerate link failures and also be capable of surviving various attacks mounted on it. It should be able to provide the guaranteed services whenever an authorized user requires them.

Non-repudiation: Non-repudiation is a mechanism to guarantee that the sender of a message cannot later deny having sent the message and that the recipient cannot deny having received the message. Digital signatures, which function as unique identifiers for each user, much like a written signature, are used commonly for this purpose.

Authentication: Enables a node to ensure the identity of the peer node it is communicating with. Without authentication, an adversary could masquerade a node, thus gaining unauthorized access to resource and sensitive information so it is interfering with the operation of other nodes. [2]

Issues And Challenges For Security

Hao yang [3] covers basic challenge and issues related to secure routing. Designing a foolproof security protocol for ad hoc wireless is a very challenging task. This is mainly because of certain unique characteristics of ad hoc wireless networks, namely, shared broadcast radio channel, insecure operating environment, lack of central authority, lack of association among nodes, limited availability of

resources, and physical vulnerability. A detailed discussion on how each of the above mentioned characteristics causes difficulty in providing security in ad hoc wireless networks is given below.

Issues And Challenges For MANET Security

Shared broadcast radio channel: Unlike in wired networks where a separate dedicated transmission line can be provided between a pair of end users, the radio channel used for communication in ad hoc wireless networks is broadcast in nature and is shared by all nodes in the network. Data transmitted by a node is received by all nodes within its direct transmission range. So a malicious node could easily obtain data being transmitted in the network. This problem can be minimized to a certain extent by using directional antennas.

Insecure operational environment: The operating environments where ad hoc wireless networks are used may not always be secure. One important application of such networks is in battlefields. In such applications, nodes may move in and out of hostile and insecure enemy territory, where they would be highly vulnerable to security attacks.

Lack of central authority: In wired networks and infrastructure-based wireless important central points (such as routers, base stations, and access points) and implement security mechanisms at such points. Since ad hoc wireless networks do not have any such central points, these mechanisms cannot be applied in ad hoc wireless networks.

Lack of association: Since these networks are dynamic in nature, a node can join or leave the network at any point of the time. If no proper authentication mechanism is used for associating nodes with a network, an intruder would be able to join into the network quite easily and carry out his/her attacks.

Limited resource availability: Resources such as bandwidth, battery power, and computational power (to a certain extent) are scarce in ad hoc wireless networks. Hence, it is difficult to implement complex cryptography-based security mechanisms in such networks.

Physical vulnerability: Nodes in these networks are usually compact and handheld in nature. They could get damaged easily and are also vulnerable to theft. [2]

Issues And Challenge For Routing In MANET Security

Detection of malicious node Node is participant in route and do the misuse of information.

Guarantee of correct route discovery We have to check the correctness of route.

Confidentiality of network topology Topology discover by malicious node so it create traffic or DOS attack.

Stability against attacks one node first participant in network. After some time it is work as a malicious node and disturb the routing process. Node must be stable not change the state.

Security Scheme

There are two main approaches in securing ad hoc environments currently utilized.

The first approach is the intrusion detection approach that aims in enabling the participating nodes to detect and avoid malicious behaviour in the network without changing the underlined routing protocol or the underling infrastructure. Although the intrusion detection field and its applications are widely researched in infrastructure networks it is rather new and faces greater difficulties in the context of ad hoc networks.

The second approach is secure routing that aims in designing and implementing routing protocols that have been designed from scratch to include security features. Mainly the secure protocols that have been proposed are based on existing ad hoc routing protocols like AODV and DSR but redesigned to include security features. In the following sub sections we briefly present the two approaches in realizing security schemes that can be employed in ad hoc networking environments.

Intusion Detection System (IDS)

Intrusion is defined as "any set of actions that attempt to compromise the integrity, confidentiality, or availability of a resource". Intrusion protection techniques works as the first line of defense. However, intrusion protection alone is not sufficient since there is no perfect security in any system, especially in the field of ad hoc networking due to its fundamental vulnerabilities.

Therefore, intrusion detection can work as the second line of protection to capture audit data and perform traffic analysis to detect whether the network or a specific node is under attack. The two type of nodes are in under attack on a network. [8]

Selfish nodes: It doesn't cooperate for selfish reasons, such as saving power. Even though the selfish nodes do not intend to damage other nodes, the main threat from selfish nodes is the dropping of packets, which may affect the performance of the network severely.

Malicious nodes: It has the intention to damage other nodes, and battery saving is not a priority. Without any incentive for cooperating, network performance can be severely degraded.

Once an intrusion has been detected then measures can be taken to minimize the damages or even gather evidence to inform other legitimate nodes for the intruder and maybe launch a countermeasure to minimize the effect of the active attacks.

Stand Alone IDS

In this architecture, each host has a IDS and detect attacks independently. There is no cooperation between nodes and all decision is based on local nodes (Figure 1). This architecture is not effective enough but can be utilized in an environment where not all nodes are capable of running IDS

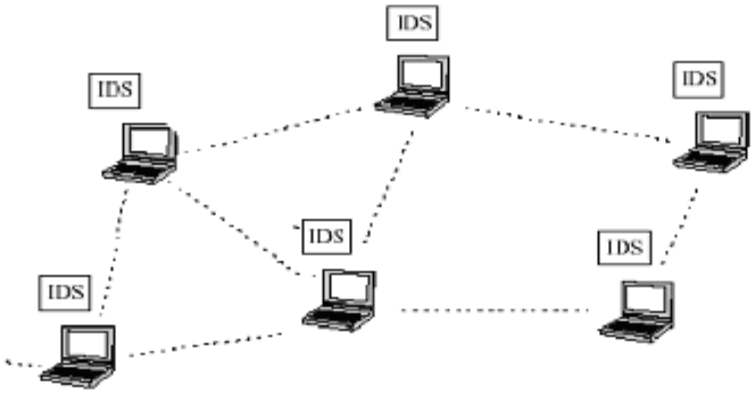

Figure 1: Stand Alone Architecture

Mechanism

Xia Wang [11] describes the various IDS system with different mechanism that used for detection of node.

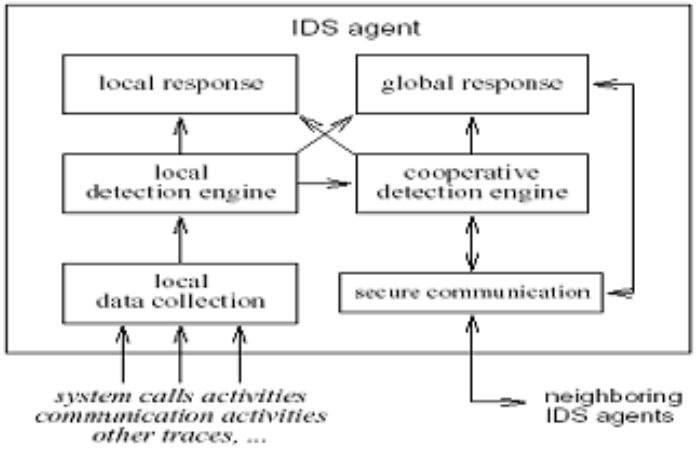

Figure 2: Distributed and cooperative architecture component

In the IDS system the mechanism is used to identify or detect the node in network. The different mechanisms are used with different architecture and according to different routing protocol mechanism is change. We have to first check that which architecture used in network for IDS and also which routing protocol is used in network In that stand alone architecture we are using Watchdog and Pathrater.[12]

Watchdog

The watchdog and pathrater scheme consists of two extensions to the DSR routing protocol that attempt to detect and mitigate the effects of nodes that do not forward packets although they have agreed to do so. This misbehavior may be due to malicious or selfish intent, or simply the result of resource overload. Although the specific methods proposed build on top of DSR. The watchdog extension is responsible for monitoring that the next node in the path forwards data packets by listening in promiscuous mode. It identifies as misbehavior nodes the ones that fail to do so.

Every node that participates in the ad hoc network employs the watchdog functionality in order to verify that its neighbors correctly forward packets. When a node transmits a packet to the next node in the path, it tries to promiscuously listen if the next node will also transmit it. Furthermore, if there is no link encryption utilized in the network, the listening node can also verify that the next node did not modify the packet before transmitting it.

The watchdog of a node maintains copies of recently forwarded packets and compares them with the packet transmissions overheard by the neighboring nodes. Positive comparisons result in the deletion of the buffered packet and the freeing of the related memory. If a node that was supposed to forward a packet fails to do so within a certain timeout period, the watchdog of an overhearing node increments a failure rating for the specific node.

This effectively means that every node in the ad hoc network maintains a rating assessing the reliability of every other node that it can overhear packet transmissions from. A node is identified as misbehaving when the failure rating exceeds a certain threshold bandwidth. The source node of the route that contains the offending node is notified by a message send by the identifying watchdog. [5]

Watchdog example

In given figure 3 is a packet is traveling from S to D. A can overhear B and tell whether B has forwarded the packet. Buffer is maintained for recently sent packets. The overheard packet is compared with the sent packet. If there is a match, discard the packet. If the packet stays till a timeout, increment the failure tally for the node. If tally exceeds a threshold, declare the node as misbehaving.[1].

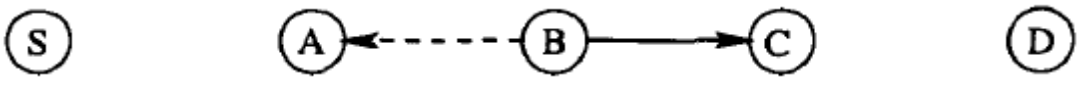

Figure 3: A Example of WatchDog

Pathrater

The pathrater assesses the results of the watchdog and selects the most reliable path for packet delivery. One of the base assumptions of this scheme is that malicious nodes do not collude in order to circumvent it and perform sophisticated attacks against the routing protocol.

The pathrater extension to DSR selects routes for packet forwarding based on the reliability rating assigned by the watchdog mechanism. Specifically, a metric for each path is calculated by the pathrater by averaging the reliability ratings of the nodes that participate in the path. This path metric allows the pathrater to compare the reliability of the available paths, or to emulate the shortest path algorithm when no reliability ratings have been collected. The pathrater selects the path with the highest metric when there are multiple paths for the same destination node.

The algorithm followed by the pathrater mechanism initially assigns a rating of 1.0 to itself and 0.5 to each node that it knows through the route discovery function. The nodes that participate on the active paths have their ratings increased by 0.01 at periodic intervals of 200 milliseconds to a maximum rating of 0.8. A rating is decremented by 0.05 when a link breakage is detected during the packet forwarding process to a minimum of 0.0. The rating of -100 is assigned by the watchdog to nodes that have been identified as misbehaving. When the pathrater calculates a path value as negative this means that the specific path has a participating misbehaving node.

The watchdog and pathrater extensions facilitate the identification and avoidance of misbehaving nodes that participate in the routing function. The identification is based on overheard transmissions and the selection of reliable routes is based on the calculated reliability of the paths.

ACKNOWLEDGEMENT

Though only my name appears on the cover of this Report, a great many people have contributed to its production. I owe my gratitude to all those people who have made this dissertation possible and because of whom my Dissertation experience has been one that I will cherish forever.

I am extremely grateful to my coordinator **Mr. Gardas Naresh Kumar (C-DAC)** for being a source of inspiration and for their constant support in the Design and Evaluation of the Dissertation. They have been the constant constructive force throughout my pursuit of Masters Degree at GTU-CDAC and I am sure that their active and passive teachings will always inspire me throughout my life.

I will always remain indebted to my guide at Shankersinh Vaghela Bapu Institute of Technology, Gandhinagar, Honorable **to Mr. Nitin Pandya.** I am thankful to him for him constant constructive criticism and invaluable suggestions, which benefited me a lot while doing research on Detection Of Malicious Nodes In Routing Of Mobile AdHoc Network. He has been always there to support me whenever I felt down or lost my way and always led me on right path.

I also express my gratitude to **Mr. Bhadreshsinh Gohil (GTU PG School)**, for providing me the infrastructure to carry out the Dissertation and to all staff members who were directly and indirectly instrumental in enabling us to stay committed.

I would like to thank my parents & my friends for always giving me full support, inspiring advices and courage to always follow righteous path whenever my steps have faltered.

CONCLUSION

After doing parametric study for different architecture of IDS system for adhoc wireless network we get the different mechanism to detect the malicious or selfish node. On that Watchdog is used in Stand Alone architecture for detect in malicious or selfish node. In Distributed and Cooperative architecture we have CONFIDANT Protocol, Probing algorithm mechanism used for detection. Stand Alone architecture Watchdog mechanism made for forwarded packet drop misbehavior done by node.

REFERENCES:

[1] S. Martiet, "Mitigating routing misbehavior in mobile ad hoc networks," ACM Mobicom, pp. 255–65, Auguest 2000.

[2] C. Murthy and B. Manoj, Ad Hoc Wireless Networks: Architectures and Protocols. New Delhi: Prentice Hall India, second ed., 2005.

[3] H. yang, "Security in mobile ad hoc networks: Challenges and solutions," IEEE Wireless Communications magazine, October 2000.

[4] K. Inkinen, "New secure routing in ad hoc networks," tech. rep., Helsinki University of Technology. kai.inkinen@hut.fi.

[5] D. O. Patroklos G. Argyroudis, "Secure routing for mobile ad hoc networks,"

[6] E. J. Caballero, "Vulnerabilities of intrusion detection systems in mobile ad-hoc networks - the routing problem," erjica@gmail.com.

[7] B. A. Jean-Marie Orset and A. Cavalli, "An efsm-based intrusion detection system for ad hoc networks," Institut National des Telecommunications GET-INT. Evry, France fjean-marie.orset, baptiste.alcalde, ana.cavallig@int-evry.fr.

[8] S. S. Frank Kargl, Andreas Klenk and M. Weber, "Advanced detection of selfish or malicious nodes in ad hoc networks," Auguest 2004.

[9] R. D. Ningrinla Marchang, "Intrusion detection system for wireless networks," Collaborative techniques for intrusion detection in mobile ad-hoc networks, pp. 508–523, June 2008.

[10] Y. X. G. S. Bo Sun, Osborne L, "Intrusion detection techniques in mobile ad hoc and wireless sensor networks," Wireless Communications, IEEE, vol. 14, pp. 56–63, October 2007.

[11] X. Wang, "Intrusion detection techniques in wireless ad hoc networks," Computer Software and Applications Conference, vol. 2, pp. 347–349, Sepetemer 2006. COMPSAC apos;06. 30th Annual International.

[12] T. W. Mike Just, Evangelos Kranakis, "Resisting malicious packet dropping in wireless ad hoc networks,"