Detection of Malicious Nodes in Mobile Adhoc Network

Vijendra Pratap Singh[1] & Sanjay Sachan[2]

s

ABSTRACT

Mobile Ad hoc Networks (MANET) consists of mobile nodes so the network topology may change rapidly and unpredictably over time. The nodes themselves execute all the network activity including discovering network topology and delivering routing messages i.e. the network is decentralized so one or more of them may behave and disturb the network. The node can cause disturbance in the network by exhibiting selfishness or misbehavior. Intrusion Detection System (IDS) is developed to detect selfish or malicious node. It has different architecture. One is Stand Alone architecture and other is Distributed and co-operative architecture. Standalone Architecture uses Watchdog 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. By using the both these mechanisms with DSR protocol provides better security in routing of ad hoc network.
Multiple hops may be required for nodes to communicate across the ad hoc network due to limited transmission range. Routing functionality is incorporated into each host, so ad hoc networks have dynamic, multi-hop, and constantly changing topologies.

All the participating nodes in mobile ad hoc network have to perform routing traffic to maintain connectivity between nodes. If they deny participating in the routing process, the connectivity may be lost and the network could be segmented.

The routing protocols that are currently utilized in ad hoc environments have specifically been designed to handle node mobility and rapidly changing topologies

Keywords

DSR (Dynamic Source Routing), IDS (Intrusion Detection System), Watchdog, Path rater

[1] M.TECH Scholar, AIET LUCKNOW, Uttar Pradesh, India, Vijendrasing@gmail.com

[2] Asst. professor, AIET LUCKNOW, Uttar Pradesh, India, sanjay.sachan@gmail.com

1. INTRODUCTION

A **mobile ad-hoc network** (**MANET**) is a self-configuring infrastructure less network of mobile nodes connected by wireless links. Infrastructure less mobile network has no fixed routers and base stations. Figure 1.1 illustrates an example ad hoc network.

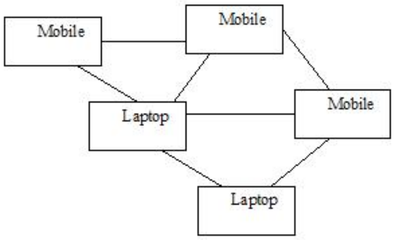


Fig 1.1: Example of Ad Hoc Network

1.1.1 TABLE DRIVEN ROUTING PROTOCOL

These protocols maintain different tables to store routing information from each node to every other node in the network and also update the routing information. Examples of the protocols of this class are, Destination Sequenced Distance Vector routing protocol (DSDV), Wireless Routing Protocol (WRP), Cluster-Head Gateway Switch Routing protocol and Source Tree Adaptive Routing protocol (STAR).

1.1.2 ON DEMAND ROUTING PROTOCOL

It eliminates maintaining routing tables for each node and updating them. It creates routes when required .When source want to send data to destination, it calls the following procedures: Route discovery, Route maintenance, Route deletion. Examples of the protocols of this class are, Dynamic Source Routing protocol (DSR), Ad Hoc On-Demand

Distance-Vector Routing protocol (AODV), and Temporally Ordered Routing Protocol (TORA).

1.1.2.1 DSR (DYNAMIC SOURCE ROUTING)

DSR is an on demand source routing protocol. It is referred to as "On Demand" because route paths are determined when a source sends a packet to a destination for which the source has no path. The two main functions of DSR is route discovery and route maintenance. Figure1.2 illustrate route discovery.

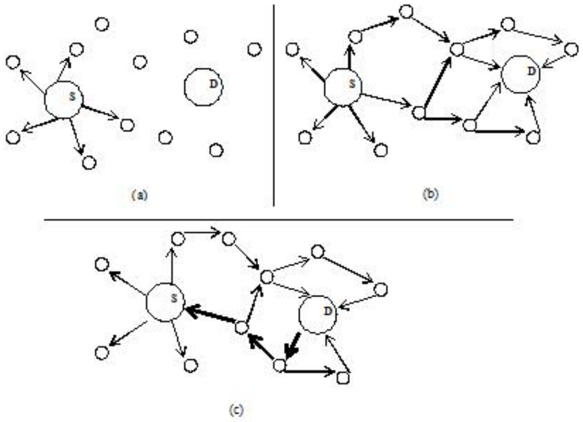
Node S (the source) wants to communicate with node D (the destination) but have no paths to D. S initiates a route discovery by broadcasting the ROUTE Request packet to its neighbors that contains the address D. The neighbors in turn append their own addresses to the ROUTE Request packet. D must now send back a route reply packet to inform S of the discovered route. Since the Route Request packet that reaches D contains a path from S to D, D may choose to use the reverse path to send back reply or to initiate a new request discovery back to S. Since there can be many routes from a source to a destination, a source may receive multiple route replies from destination. DSR caches these routes in a route cache for future use.

Figure 1.2a) Sender broadcasts route request (b) Intermediate nodes stamp and forward request (c) Destination sends a (source routed) reply containing path

The second function is route maintenance that manages link breaks. When a path has two nodes which are not in transmission range then link break occurs. While forwarding a packet to the next node in the route path, if an intermediate node detects link break it sends back a message to source notifying it of that link break. Then, the source must try another path or do a route discovery.

1.1.3 HYBRID ROUTING PROTOCOL

It introduces comparison between the table driven routing protocols and on-demand routing protocols. Table driven



mechanism is applied for routing inside a single zone and on-demand routing is done beyond the zone boundaries. There is less delay in route setup process in table driven routing protocols due to availability of routing information than on-demand routing protocols. Table driven routing protocols costs higher signaling traffic than required for on-demand routing protocols. There are some variations the two classes of protocol for functions like path configuration after link failures. So, we cannot draw any preference conclusions at the protocol level.

2. NETWORK SECURITY

A security protocol should satisfy the following requirements for ad hoc wireless networks:

Confidentiality: The data sent by the sender (source node) must be comprehensible only to the intended receiver (destination node).Data encryption is one of the popular techniques for ensuring confidentiality.

Integrity: It should not be possible for any malicious node in the network to tamper with the data sent by the source node to the destination node.

Availability: The network should be operational all the time. It must be robust enough to tolerate link failures. It should provide the guaranteed services whenever an authorized user requires them.

Non-repudiation: This mechanism ensures 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 are used for this purpose.

Authentication: It 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 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].

3. ISSSUES AND CHALLENGES FOR MANET SECURITY

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[3].

Shared broadcast radio channel: The

radio channel used for communication in ad hoc wireless networks is broadcast in nature and is shared by all nodes in the network.

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, where nodes may move in and out of hostile and insecure enemy territory and they would be highly vulnerable to security attacks.

Lack of Central authority: In wired networks and infrastructure-based **networks**, it is possible to monitor the traffic on the network through certain control points (such as base stations, routers and access points) and implement security mechanisms at such points. These mechanisms cannot be applied in ad hoc wireless networks since they do not have any such central points.

Lack of association: A node can join or leave the network at any point of the time since these networks are dynamic in nature.

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

Physical vulnerability: Nodes are compact and handheld in nature. They could get damaged easily and are also vulnerable to theft.

4. NETWORK SECURITY ATTACKS

Attacks on ad hoc wireless networks can be classified into two broad categories, namely**, Passive and Active attacks [4].**

Passive attack does not disrupt the operation of the network. The adversary snoops the data exchanged in the network without altering it. One way of overcoming such problems is to use powerful encryption mechanisms.

Active attack attempts to alter or destroy the data being exchanged in the network. Active attacks can be classified further into two categories, namely, **External and Internal attacks.**

External attacks are carried out by nodes that do not belong to the network.

Internal attacks are from compromised nodes that are actually part of the network.

4.1 INTERNAL ATTACK

WORMHOLE: The wormhole attack involves the cooperation between two malicious nodes that participate in the network. One attacker, say node A, captures routing traffic at one point of the network and tunnels them to another point in the network, say to node B, that shares a private communication link with A. Node B then selectively injects tunneled traffic back into the network (see Figure 1.3).The connectivity of the nodes that have established routes over the wormhole link is completely under the control of the two colluding attackers. [5]

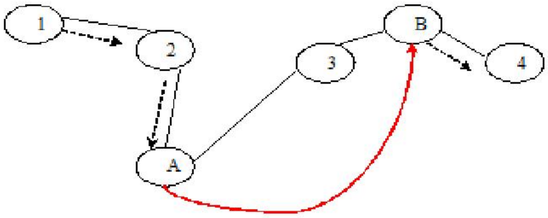


Figure 1.3: A wormhole attack performed by colluding malicious nodes A and B.

Black hole: In a black hole attack a malicious node injects false route replies to the route requests it receives advertising itself as having the shortest path to a destination. These fake replies can be fabricated to divert network traffic through the malicious node for eavesdropping, or simply to attract all traffic to it in order to perform a denial of service attack by dropping the received packets. [6]

Byzantine attack: A set of compromised intermediate nodes works in collusion and carry out attacks such as creating routing loops, forwarding packets through non-optimal paths, or selectively dropping packets, which results in disruption or degradation of the routing services.

Resource consumption attack: This is also known as the sleep deprivation attack. An attacker or a compromised node can attempt to consume battery life by requesting excessive route discovery, or by forwarding unnecessary packets to the victim node.

4.2 ROUTING ATTACK

Routing attack is done by the attacker [4].

Routing table overflow attack: The proactive routing algorithms are more vulnerable to table overflow attacks because proactive routing algorithms attempt to discover routing information before it is actually needed. An attacker can simply send excessive route advertisements to overflow the victim's routing table.

Routing cache poisoning attack: In route cache poisoning attacks, attackers take advantage of the promiscuous mode of routing table updating, where a node overhearing any packet may add the routing information contained in that packet header to its own route cache, even if that node is not on the path.

Rushing attack: If a fast transmission path (e.g. a dedicated channel shared by attackers) exists between the two ends of the wormhole, the tunneled packets can propagate faster than those through a normal multi-hop route. This forms the rushing attack.

Replay: An attacker that performs a replay attack injects into the network routing traffic that has been captured previously.

Denial of service: Denial of service attacks aim at the complete disruption of the routing function and therefore the whole operation of the ad hoc network.

Man in middle attack: An attacker sits between the sender and the receiver sniffs any information being sent between two ends. In some cases the attacker may impersonate the sender to communicate with the receiver, or impersonate the receiver to reply to the sender. [7].

5. 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 behavior in the network without changing the routing protocol or infrastructure.

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

5.1 INTRUSION DETECTION SYSTEM (IDS)

Intrusion is defined as "any set of actions that attempt to compromise the integrity, confidentiality, or availability of a host, or to notify another participating node for the malicious action of the node that performs the attack. resource". Intrusion protection techniques captures audit data and perform traffic analysis to detect whether the network or a specific node is under attack. The two types of nodes are is under attack on a network. [8]

Selfish nodes: It doesn't cooperate for selfish reasons, such as saving power. 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.

5.1.1 IDS Architecture

An intrusion detection system (IDS) can be classified as network-based or host-based according to the audit data that is used [9] [10].

A network-based IDS runs on a gateway of a network and captures and examines the network traffic that flows through it. Obviously this approach is not suitable for ad hoc networks since there is no central point that allows monitoring of the whole network. A host-based IDS relies on capturing local network traffic to the specific host. This data is analyzed and processed locally to the host and is used either to secure the activities of this.

5.1.1.1 STAND ALONE IDS

In this architecture, each host has IDS and detects attacks independently. There is no cooperation between nodes and all decision is based on local nodes (Figure 1.4).This architecture is not effective enough but can be utilized in an environment where not all nodes are capable of running IDS.

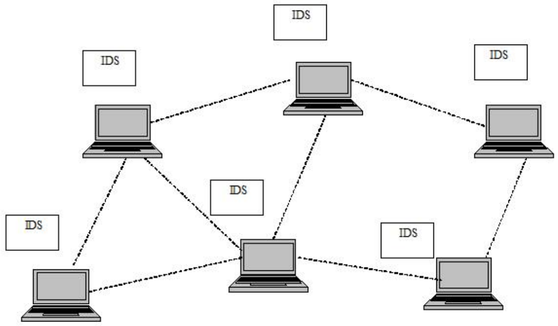


Figure 1.4: Stand Alone Architecture

5.1.1.2 DISTRIBUTED AND COOPERATIVE IDS

Intrusion detection and response systems should be both distributed and cooperative to suit the needs of mobile ad-hoc networks (Figure 1.5).

In the systems aspect, individual IDS agents are placed on each and every node. Each IDS agent runs independently and monitors local activities (including user and systems activities, and communication activities within the radio range). It detects intrusion from local traces and initiates response. If anomaly is detected in the local data, or if the evidence is inconclusive and a broader search is warranted, neighboring IDS agents will cooperatively participate in global intrusion detection actions. These individual IDS agent collectively form the IDS system to defend the mobile ad-hoc network.

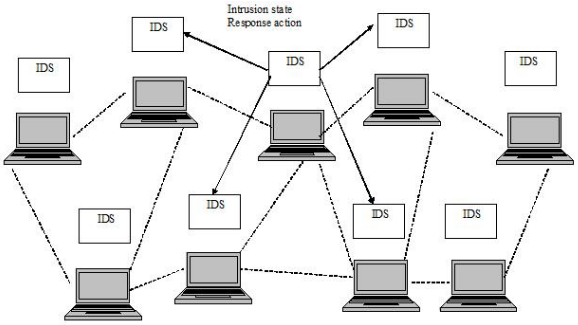
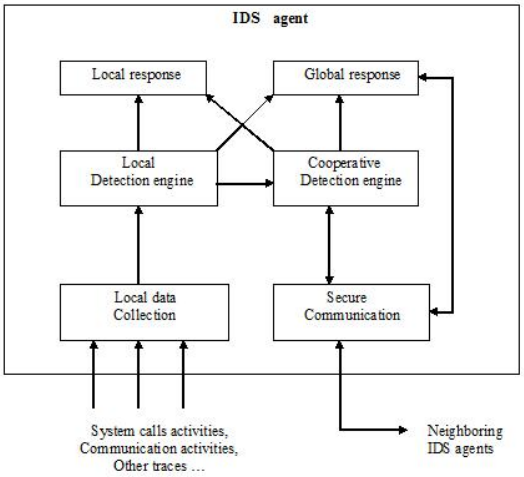
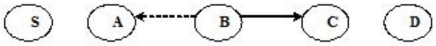


Figure 1.5: Distributed and cooperative Architecture

The internal of an IDS agent can be fairly complex, but conceptually it can be structured into six pieces (Figure 1.6).The data collection module is responsible for gathering local audit traces and activity logs. Next, the local detection engine will use these data to detect local anomaly. Detection methods that need broader data sets or that require collaborations among IDS agents will use the cooperative detection engine.

Intrusion response actions are provided by both the local response and global response modules. The local response module triggers actions local to this mobile node, for example an IDS agent alerting the local user, while the global one coordinates actions among neighboring nodes, such as the IDS agents in the network electing a remedy action. Finally, a secure communication module provides a high configuration dense communication channel among IDS agents.





Listening node verifies 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. If the result of comparisons is positive, then there is 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 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] In given figure 1.7 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 1.7: An Example of Watchdog

In given figure 3.4 are 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]

5.1.2.2 PATH RATER

The path rater extension to DSR selects the most reliable path for packet forwarding according to the reliability rating done by watchdog mechanism. It is based on the assumption that malicious nodes do not collude to perform attacks against the routing protocol. The path rater calculates a metric for each path by averaging the reliability ratings of the participating nodes in the path. This path metric allows to compare the reliability of the available paths, or to emulate the shortest path algorithm when no reliability ratings have been collected. When multiple paths are available for the same destination node, the path rater selects the path with the highest metric.

The algorithm followed by the path rater mechanism initially assigns a rating of 1.0 to itself and 0.5 to each node determined through the route discovery function. The rating of nodes on the active paths is 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 misbehaving nodes. When the path rater calculates a path value as negative this means that the specific path has a participating misbehaving node.

5.2 SECURE ROUTING

This approach attempts to design secure routing protocols for ad hoc networks. These protocols are either completely new stand-alone protocols, or in some cases incorporations of security mechanisms into existing protocols like AODV and DSR.

Generally the existing secure routing protocols that have been proposed can be broadly classified into two categories, those that use hash chains, and those that in order to operate require predefined trust relationships.

The Secure Efficient Ad hoc Distance vector routing protocol (SEAD) employs the use of hash chains to authenticate hop counts and sequence numbers. It provides loop freedom and protects the nodes from impersonation and several other attacks. Another secure routing protocol is Ariadne. Ariadne assumes the existence of a shared secret key between two nodes and uses a message authentication code (MAC) in order to authenticate point-to-point messages between nodes.

SAODV proposes a set of extensions that secure the AODV routing packets. For authenticating the non-mutable fields it uses cryptographic signatures, while one-way hash chains are used for securing every different route discovery process.

Another protocol is the Security-aware Ad hoc Routing (SAR) that extends on demand ad hoc routing protocols like AODV and DSR. The main aspect of SAR is that it introduces a new security metric in the route discovery and maintenance process.

6. ACKNOWLEDGMENTS

It gives me immense pleasure in expressing my thanks and profound gratitude to Mr. Sanjay Sachan for his valuable guidance and continuous encouragement. I am heartily thankful to him for his precious time, suggestions and sorting out the difficulties of my topic that helped me a lot during this study.

REFERENCES

[1] S. Martinet, "Mitigating routing misbehavior in mobile ad hoc networks" ACM Mobicom, pp. 255–65, August 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," Institute 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," August 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, September 2006. COMPSAC apes 06, 30th Annual International.

[12]T. W. Mike Just, Evangelos Kranakis, "Resis ting malicious packet dropping in wireless ad hoc network".