IJISET - International Journal of Innovative Science, Engineering & Technology, Vol. 2 Issue 6, June 2015.
www.ijiset.com
ISSN 2348 – 7968

Detection of Malicious Nodes in Mobile Adhoc Network

Mrinal Paliwal[1], Saddam Hussain[2]

[1,2]Department of Computer Science & Engineering

P.K. Group of Institutions Mathura, India

[1]mrinal.pali@gmail.com [2]kundan.suddu@gmail.com

Abstract-
Mobile Ad hoc Networks (MANET) comprises of versatile nodes so that system topology might change quickly and erratically over the long haul. The hubs themselves execute all the system movement including finding system topology and conveying steering messages i.e. the system is decentralized so one or a greater amount of them may carry on and aggravate the system. The hub can bring about unsettling influence in the system by showing childishness or bad conduct. Interruption Detection System (IDS) is created to recognize childish or malevolent hub. It has distinctive building design. One is Stand Alone building design and other is Distributed and co-agent structural planning. Remain solitary Architecture utilizes Watchdog component to identify childish and acting mischievously hub that consent to forward bundle yet neglects to do as such. Way rater will be system utilized for expelling way from store that contain noxious or narrow minded hub. By utilizing the both these instruments with DSR convention gives better security in directing of specially appointed system.

Keywords-
DSR (Dynamic Source Routing), IDS (Intrusion Detection System), Watchdog, Path rater, Security Attacks.

1. INTRODUCTION

Mobile Ad hoc Networks (MANET) is a self-arranging framework less system of versatile hubs associated by remote connections. *Foundation* less portable system has no altered switches and base stations. Figure 1.1 represents an illustration

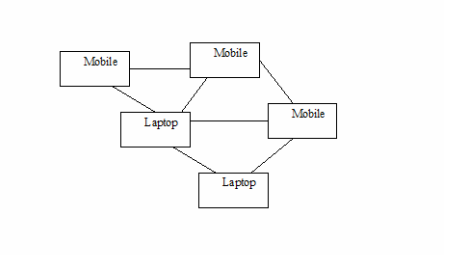

Fig 1.1: Example of Ad Hoc Network

Various hops may be obliged for hubs to impart over the ad hoc organize because of constrained transmission range. Routing usefulness is joined into every host, so ad hoc systems have dynamic, multi-bounce, and continually evolving topologies.
All the taking an interest hubs in versatile ad hoc system need to perform routing movement to keep up integration between hubs. On the off chance that they deny taking an interest in the routing process, the network may be lost and the system could be divided.
The routing protocols that are as of now used in ad hoc situations have particularly been intended to handle hub portability and quickly changing topologies.

1.1 Routing of Ad hoc Network

In ad hoc system, the routing protocol keeps up a routing table with data applicable to which the following bounce for this parcel ought to be keeping in mind the end goal to achieve its destination. Routing protocols for Ad Hoc systems administration can be ordered into four classifications viz. taking into account the routing data upgrade system, the utilization of worldly data for routing, routing topology, and usage of particular assets.

1.1.1 Table Driven Routing Protocol

These protocols keep up diverse tables to store routing data from each hub to each other hub in the system furthermore overhaul the routing data. Illustrations of the protocols of this class will be, 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 wipes out keeping up routing tables for every hub and overhauling them. It makes courses when obliged .When source need to send information to destination, it calls the accompanying methodology: Route disclosure, Route support, Route erasure. Samples of the protocols of this class are, Dynamic Source Routing protocol (DSR), Ad Hoc On-Demand Separation Vector Routing protocol (AODV), and Temporally Ordered Routing Protocol (TORA).

ISSN 2348 – 7968

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.

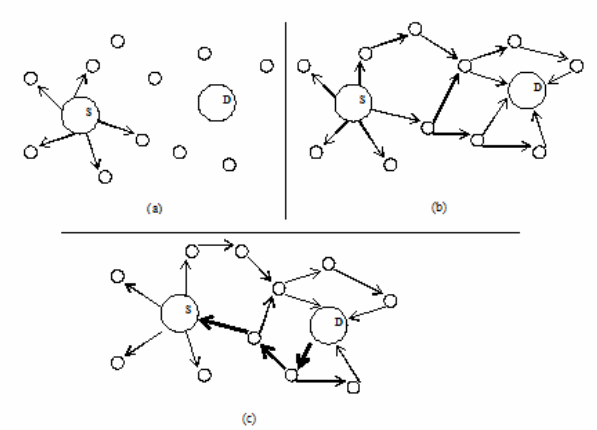

Figure 1.2(a) Sender broadcasts route request (b) Intermediate nodes stamp and forward request (c) Destination sends a (source routed) reply containing path

The second capacity is course support that oversees connection breaks. At the point when a way has two hubs which are not in transmission run then connection break happens. While sending a bundle to the following hub in the course way, if a halfway hub distinguishes connection crush it sends spirit a message to source informing it of that join break. At that point, the source must attempt another way or do a course disclosure.

1.1.3 Hybrid Routing Protocol

It presents correlation between the table driven routing protocols and on-interest routing protocols. Table driven instrument is requested routing inside a solitary zone and on- interest routing is done past the zone limits. There is less postpone in course setup handle in table driven routing protocols because of accessibility of routing data than on- request routing protocols. Table driven routing protocols costs higher flagging activity than obliged for on-interest routing protocols. There are a few varieties the two classes of protocol for capacities like way setup a great many connection disappointments. Thus, we can't make any inclination inferences 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

ISSN 2348 – 7968

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 assault includes the participation between two vindictive nodes that take an interest in the system. One assailant, say node A, catches routing activity at one purpose of the system and passages them to another point in the system, say to node B, that imparts a private correspondence connection to A. Node B then specifically infuses burrowed movement again into the system .The network of the nodes that have set up courses over the wormhole join will be totally under the control of the two plotting aggressors. [5]

Black hole: In a black hole assault a noxious node infuses false course answers to the course asks for it gets advertising itself as having the briefest way to a destination. These fake answers can be created to redirect system activity through the vindictive node for spying, or essentially to pull in all movement to it to perform a refusal of administration assault by dropping the got bundles. [6]

Byzantine attack: An arrangement of bargained middle of the road nodes meets expectations in agreement and complete assaults such as making routing circles, sending parcels through non-ideal ways, or specifically dropping bundles, which brings about interruption or degradation of the routing administrations.

Resource consumption attack: This is otherwise called the lack of sleep assault. An aggressor or a bargained node can endeavor to devour battery life by asking for unreasonable course revelation, or by sending superfluous parcels to the casualty node.

ISSN 2348 – 7968

4.2 Routing Attack

Routing attack is done by the attacker [4].

Routing table overflow attack: The proactive routing calculations are more powerless against table flood assaults in light of the fact that proactive routing calculations endeavor to find routing data before it is really required. An aggressor can essentially send over the top course advertisements to flood the casualty's routing table.

Routing cache poisoning attack: In course store harming assaults, assailants exploit the unbridled method of routing table overhauling, where a node catching any bundle may add the routing data contained in that parcel header to its own course reserve, regardless of the possibility that that node is not on the way.

Rushing attack: On the off chance that a quick transmission way (e.g. a committed channel shared by aggressors) exists between the two closures of the wormhole, the burrowed bundles can proliferate speedier than those through a typical multi-jump course. This shapes the hurrying assault.

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 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 named system based or host-based by review information that is utilized [9] [10].

A system construct IDS keeps running with respect to an entryway of a system and catches and looks at the system movement that moves through it. Clearly this methodology is not suitable for ad hoc systems since there is no essential issue that permits checking of the whole system.

A host-construct IDS depends with respect to catching nearby system movement to the particular host. This information is investigated and handled generally to the host and is utilized either to secure the exercises of this host, or to tell another taking part node for the noxious activity of the node that performs the assault.

5.1.1.1 Stand Alone IDS

In this structural engineering, every host has IDS and identifies assaults autonomously. There is no participation in the middle of nodes and all choice is in view of neighborhood nodes (Figure 1.4).This building design is not sufficiently compelling but rather can be used in a situation where not all nodes are equipped for running IDS.

ISSN 2348 – 7968

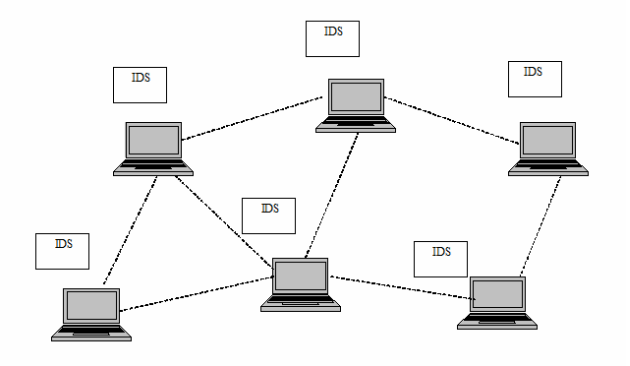

Figure 1.4: Stand Alone Architecture

5.1.1.2 Distributed and Co-operative IDS

Intrusion detection and reaction systems ought to be both conveyed and agreeable to suit the needs of versatile ad- hoc systems (Figure 1.5).

In the systems angle, singular IDS operators are put on every last node. Every IDS specialists runs freely and screens nearby exercises (counting client and systems exercises, and correspondence exercises inside the radio reach). It identifies intrusion from neighborhood follows and starts reaction. On the off chance that abnormality is distinguished in the nearby information, or if the confirmation is uncertain and a broader pursuit is justified, neighboring IDS specialists will agreeably take part in worldwide intrusion detection activities. These individual IDS operators all in all shape the IDS system to safeguard the versatile ad-hoc system.

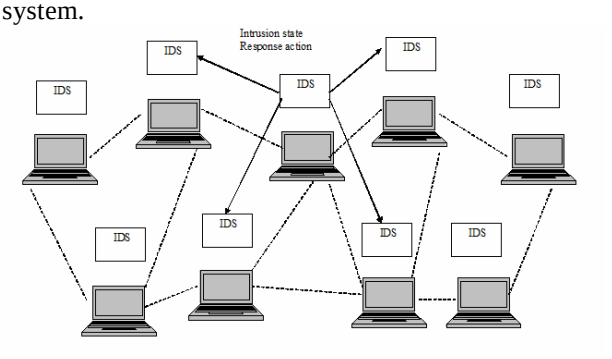

Figure 1.5: Distributed and cooperative Architecture

The inward of an IDS operators can be genuinely perplexing, yet thoughtfully it can be organized into six pieces

(Figure1.6).The information accumulation module is in charge of gatheringlocal review follows and movement logs. Next, the nearby detection motor will utilize these information to recognize neighborhood abnormality. Detection systems that need broader information sets or that oblige coordinated efforts among IDS specialists will utilize the helpful detection motor.

Intrusion reaction activities are given by both the neighborhood reaction and worldwide reaction modules. The nearby reaction module triggers activities neighborhood to this versatile node, for instance an IDS operators alarming the nearby client, while the worldwide one directions activities among neighboring nodes, such as the IDS specialists in the system choosing a cure activity. At long last, a protected correspondence module gives a high design thick correspondence channel among IDS operators.

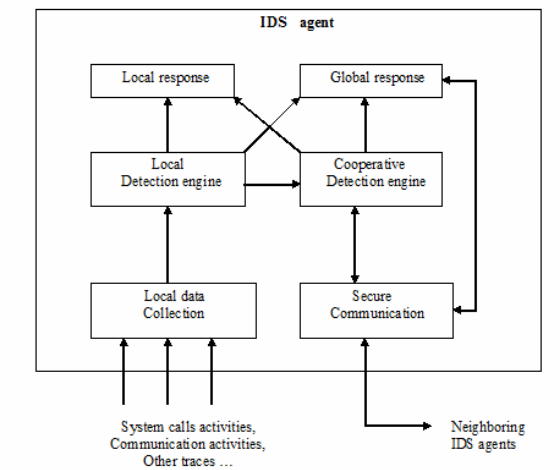

Figure 1.6: Distributed and cooperative architecture component

5.1.2 Mechanism

The various IDS system use different mechanisms for detection of node [11]. According to different routing protocol mechanisms change. We have to first check that which architecture used in network for IDS and also which routing protocol is used in network. In the stand alone architecture we use Watchdog and Path rater. [12]

5.1.2.1 WATCHDOG

The watchdog expansion screens that the following node in way advances information bundles by listening in unbridled mode. Each node in the ad hoc system utilizes watchdog usefulness to check that its neighbors forward parcels accurately. Amid transmission of bundles, a node

ISSN 2348 – 7968

tries to indiscriminately listen if the following node will likewise transmit it. On the off chance that there will be no join encryption used in the system, the listening node confirms that the following node did not change the parcel before transmitting it.

The watchdog of a node keeps up duplicates of as of late sent bundles and contrasts them and the parcel transmissions caught by the neighboring nodes. In the event that the aftereffect of correlations is positive, then there is cancellation of the cushioned bundle and the liberating of the related memory. On the off chance that a node that should forward a parcel neglects to do as such inside of a certain timeout period, the watchdog of a catching node increases a disappointment rating for the particular node A node is recognized as getting out of hand when the disappointment rating surpasses a certain limit data transfer capacity. The source node of the course that contains the culpable node is informed by a message send by the distinguishing watchdog. [5] In given figure 1.7 is a parcel is making a trip from S to D. A can catch B and tell whether B has sent the parcel. Support is kept up for as of late sent parcels. The caught bundle is contrasted and the sent parcel. On the off chance that there is a match, toss the parcel. In the event that the bundle stays till a timeout, increase the disappointment count for the node.If count surpasses an edge, announce the node as misbehaving.[1]

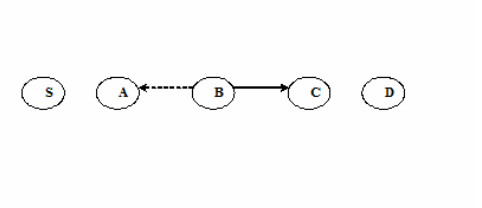

Figure 1.7: An Example of Watchdog

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 watchdog expansion screens that the following node in way advances information bundles by listening in unbridled mode. Each node in the ad hoc system utilizes watchdog usefulness to check that its neighbors forward parcels accurately. Amid transmission of bundles, a node

tries to indiscriminately listen if the following node will likewise transmit it. On the off chance that there will be no join encryption used in the system, the listening node confirms that the following node did not change the parcel before transmitting it.

The watchdog of a node keeps up duplicates of as of late sent bundles and contrasts them and the parcel transmissions caught by the neighboring nodes. In the event that the aftereffect of correlations is positive,then there is cancellation of the cushioned bundle and the liberating of the related memory. On the off chance that a node that should forward a parcel neglects to do as such inside of a certain timeout period, the watchdog of a catching node increases a disappointment rating for the particular node A node is recognized as getting out of hand when the disappointment rating surpasses a certain limit data transfer capacity. The source node of the course that contains the culpable node is informed by a message send by the distinguishing watchdog. [5] In given figure 1.7 is a parcel is making a trip from S to D. A can catch B and tell whether B has sent the parcel. Support is kept up for as of late sent parcels. The caught bundle is contrasted and the sent parcel. On the off chance that there is a match, toss the parcel. In the event that the bundle stays till a timeout, increase the disappointment count for the node.If count surpasses an edge, announce the node as misbehaving.[1]

5.2 Secure Routing

This methodology endeavors to plan secure routing protocols for ad hoc systems. These protocols are either totally new remain solitary protocols, or sometimes consolidations of security systems into existing protocols like AODV and DSR.

By and large the current secure routing protocols that have been proposed can be broadly grouped into two classifications, those that utilization hash chains, and those that with a specific end goal to work oblige predefined trust connections.

The Secure Efficient Ad hoc Distance vector routing protocol (SEAD) utilizes the utilization of hash ties to validate bounce numbers and succession numbers. It gives circle flexibility and shields the nodes from mimic and a few different assaults. Another secure routing protocol is Ariadne. Ariadne expect the presence of a common mystery key between two nodes and uses a message verification code (MAC) keeping in mind the end goal to confirm point-to-point messages between nodes.

SAODV proposes an arrangement of augmentations that protected the AODV routing parcels. For verifying the non-alterable fields it utilizes cryptographic marks, while one-way hash chains are utilized for securing each diverse course disclosure process.

Another protocol is the Security-mindful Ad hoc Routing (SAR) that reaches out on interest ad hoc routing protocols like AODV and DSR. The primary part of SAR is that it presents another security metric in the course revelation and upkeep process.

ISSN 2348 – 7968

6. ACKNOWLEDGMENTS

It gives me colossal delight in communicating my thanks and significant appreciation to Mr.Vijendra Pratap Singh for his profitable direction and persistent consolation. I am healthily grateful to him for his valuable time, proposals and dealing with the troubles of my theme that helped me a great deal amid this study.

7. REFERENCE

[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
200
7.

[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, "Resisting malicious packet dropping in wireless ad hoc networ