ISSN: 2321-7782 (Online)
Volume 2, Issue 9, September 2014
International Journal of Advance Research in Computer Science and Management Studies
Research Article / Survey Paper / Case Study
Available online at: www.ijarcsms.com

Efficient Detection and Prevention of Impersonation attack in MANET

Nidhi Gour[1]
M.Tech Scholar, CSE Dept
JECRC University
Jaipur – India

Ajay Kumar[2]
Assistant Professor, CSE Dept
JECRC University
Jaipur – India

Abstract: ***To avoid the Impersonation assault in system the encryption and unscrambling that is cryptographic procedures are emulated. On the other hand, the cryptographic validation may not be constantly appropriate in view of the constrained assets on remote gadgets and needing of a settled key administration framework in the remote system. Proposed framework uses an unsupervised thresholding methodology to discover an ideal edge to parcel the RSS hint of a hub character into two classes. Given the RSS is uniquely associated to a remote hub's physical area, the parceled two classes will be exceptionally connected if there is no mocking assaults, while less or not related when a caricaturing assault is available. This proposed framework utilizes the got signal quality (RSS)-based spatial correspondence, a physical property connected with every remote hub that is difficult to adulterate and not dependent on cryptography as the premise for catching mocking assaults.***

I. INTRODUCTION

Versatile Ad-hoc Network is self designed structure accumulation of portable hubs that impart to one another by sending parcels inside its sure radio extent though others hubs require the assistance of middle hubs to course their bundles. Versatile phone, laptop, PC, individual Digital Assistance are incorporated in hubs. Portable specially appointed system offers speedy and level system sending in conditions where it is unrealistic overall. Specially appointed is a Latin word, which signifies "for this or for this just."

The switches, the taking part hubs go about as switch, are allowed to move arbitrarily and oversee themselves subjectively therefore; the system's remote topology may change quickly and erratically. Such a system may work in a standalone design, or may be joined with the bigger Internet. To make a course between hubs directing conventions are locked in.

Routing protocols are partitioned into three classifications in MANET first is Proactive or table driven in which course are settled and immediately joined with hubs for team up, courses are upgraded in every association. Second is Reactive or on demand protocol in which association create when they are required if course is not accessible to end hub it launch course disclosure process until course made him accessible. Third one is hybrid protocol that is fusion of both proactive and reactive conventions.

Optimized Link State directing (OLSR) and Destination Sequenced Distance Vector Routing (DSDV) conventions are proactive steering conventions. Especially Ad-hoc On demand Distance Vector (AODV) and Dynamic Source Routing (DSR) conventions are receptive conventions. AODV is similarly secure steering convention that is conveying generally in remote correspondence framework.

II. AODV

Specially Ad-hoc On Demand Distance Vector Routing is well known directing convention in remote media. As In [2],it is a reactive protocol: hubs in the system trade steering data just when a correspondence must take place and stay up with the latest just the length of the correspondence keeps going. At the point when a hub must send a packet to an alternate hub, it begins a

course disclosure transform to secure a course around the end hub. In this way, it sends its neighbors a course ask for message (RREQ). Neighboring hubs get the demand, increase the bounce number, and forward the message to their neighbors, so RREQs are really shown utilizing a flooding methodology. The objective of the RREQ message is to discover the goal hub, however it additionally has the symptom of making different hubs take in a course towards the source hub (the converse course): a hub that has gotten a RREQ message, with source address S from its neighbor A, realizes that it can achieve S through An and records this data in its steering table alongside the bounce check. The RREQ message will inevitably achieve the objective hub, which will respond with a course answer message (RREP). The RREP is sent as an unicast, utilizing the way towards the source hub secured by the RREQ. So also to what happens with RREQs, the RREP message permits halfway hubs to take in a course around the terminus hub (i.e., the originator of the RREP). Subsequently, at the end of the course revelation process, parcels could be conveyed from the source to the terminus hub and the other way around. A third sort of directing message, called course slip (RERR), permits hubs to advise lapses, for instance, on the grounds that a past neighbor has moved and is no more reachable. On the off chance that the course is not dynamic (i.e., there is no information activity moving through it), all directing data lapses after a timeout and is expelled from the steering table.

Source address	Broadcast Id	Source Sequence number	Destination address	Destination Sequence number	Hop count

III. Security Threats in AODV

A hub is malevolent in the event that it is an aggressor that can't distinguish itself as an authentic hub because of the absence of legitimate cryptographic data. A hub is traded off in the event that it is an inside assailant who is acting vindictively however might be recognized by the system as a real hub and is trusted by different hubs. A hub is called egotistical when it has a tendency to deny it assets for the profits of different hubs with a specific end goal to spare its own particular assets. Since AODV has no security mechanisms several attacks can be launched against the AODV routing protocol [2].

Four types of attacks addressed by authors of [1] are:

a) Distributed false route request

b) Denial of service

c) Destination is compromised

d) Impersonation

a) Distributed false route request:

A route request is generated whenever a node has to send data to the particular destination. A malicious node might generate frequent, unnecessary route requests then it will be difficult to identify the malicious node.

Route request messages are broadcast messages. When the node in the network receive a number of route requests that is greater than a threshold count by a specific source for a destination in a particular time interval, the node is declared as malicious and the information is propagated in the network.

b) Denial of service:

A malicious node launches the denial of service attack by transmitting false control packets and using the entire network resources. Thereby other nodes are underprivileged of the resources. Denial of service can be launched by transmitting fake routing packets or data packets. It can be identified if a node is generating the control packets that are more than the threshold count in a particular time interval t frequency.

c) Destination is compromised:

A destination might not be able to reply, if it is (i) not in the network (ii) overloaded (iii) it did not receive route request or if it is (iv) malicious. This attack is identified when the source does not receive the reply from the destination in a particular time interval *t* wait.Besides the neighbours generate probe/ hello packets to determine connectivity. If the node is in the network and does not respond to route requests destined for it, it is identified as malicious.

d) Impersonation:

It can be avoided if sender encrypts the packet with its private key and other nodes decrypts with the public key of the sender. If the receiver is not able to decrypt the packet, the sender might be not the real source and hence packet will be dropped.

IV. IMPERSONATION ATTACKS

This sort of assault is likewise called parodying assaults in which a malignant hub utilizes IP location of an alternate hub in cordial directing parcels. The points of mimic assaults to get some secret data that ought to be kept mystery amid the correspondence. The data may incorporate the area, public key private key or even secret key of the hubs.

A defective hub or an enemy might preset numerous characters to a distributed system to show up and work as different hub. By getting to be some piece of the shared system the foe might then catch correspondence.

The presentation of mimic assault in any system there is a lessening of throughput in the system. Packet conveyance degree additionally drops and there is an expands checksum mistake and parcel misfortune degree. in cryptography and machine security is a manifestation of dynamic listening stealthily in which the assailant makes free associations with the exploited people and transfers messages between them, making them accept that they are talking straightforwardly to one another over a private association, at the point when indeed the whole discussion is controlled by the assailant.

The assailant must have the capacity to capture all messages going between the two exploited people and infuse new ones, which is clear as a rule (for instance, an aggressor inside gathering scope of a decoded Wi-Fi remote access point, can embed himself as a man-in-the-center).

A man-in-the-center assault can succeed just when the assailant can mimic every endpoint to the fulfillment of the other — it is an assault on common confirmation. So it is extremely imperative for any system to distinguish the mimic hubs and disconnect them from the system for the correct and smooth working of MANET

At the point when source send any message to distinctive centers inside the framework then that threatening center also recover that rub and mishandled all the information Impersonation strike is key driver of plotting attack in which traded off hub infused noxious hub into the system also make number of imitated duplicate of pernicious hub for doing future assaults in general system.

Existing System

In AODV, a source node initiates route discovery when it needs to communicate with a destination for which it does not have a route. Route discovery is initiated by the source node broadcasting a route request message (RREQ) that contains a request ID. If a node receives a RREQ that it has received previously, it drops the request. Otherwise, it stores the address of the node from which it received the request. In this manner, a reverse route to the source is established. If the RREQ reaches the destination node or a node that has a route to the destination, the node sends a route reply message (RREP) to the source. Intermediate nodes that do not have a path to the destination re-broadcast the request when they receive it for the first time. As the RREP is sent back to the source, each node stores the address of the node that sent the reply. The forward path determined from the source to the destination is used for sending packets to the destination. AODV uses sequence numbers maintained for the different destinations so as to guarantee freshness of routing information. AODV nodes offer connectivity information by broadcasting local Hello messages. If a node has not sent a broadcast within a specified time interval, it broadcasts a Hello message. Thus, a node can have a local table that contains all of its neighbors.

Disadvantages:

- It does not localize adversaries in the network
- It does not eliminate the adversary from the network.
- AODV protocol does not achieve the security features like authentication, confidentiality, integrity and non-repudiation.

V. PROPOSED SYSTEM

The proposed work varies from the past study that uses the spatial data to aid in assault discovery. Besides, the proposed work is novel in light of the fact that none of the leaving work can focus the quantity of assailants when there are various enemies taking on the appearance of the same character. Furthermore, the proposed methodology can precisely confine various enemies actually when the assailants differing their transmission force levels to trap the arrangement of their actual areas.

Advantages:

- It finds the attack presents in the network
- It eliminates the adversary from the network
- A security association must exist between network members; these security associations ensure authentication for trusted nodes.
- Sensitive information must be exchanged confidentially between the nodes in the network.
- Integrity of the information exchanged within the network has to be maintained so that corrupted messages are detected and blocked.

Contribution

The main proposal of the secure routing is to ensure better performance in the core of the mobile networks. To achieve secure communication in MANET, routing protocol must encapsulate an essential set of security mechanisms. These are mechanisms that help prevent, detect, and respond to security attacks. There are three major security goals that need to be addressed in order to maintain a reliable and secure ad-hoc network environment. The security of the ad hoc networks is considered from the following attributes:

Confidentiality:

It ensures that certain information is never disclosed to unauthorized entities. In the ad hoc network, not only sensitive information transmitted requires confidentiality; routing information must also remain secure in case it might be valuable for adversaries.

Integrity:

It guarantees that information being transferred is never altered. Only authorized nodes are able to modify the transferred information. Both malicious attacks and benign failure, such as radio propagation impairment could cause information corruption.

Authentication:

It enables communication parties could identify with each other. Therefore, an adversary cannot masquerade a node to gain sensitive resources.

SIMULATION MODEL

SIMULATOR	Network Simulator 2
NUMBER OF NODES	Random
TOPOLOGY	Random
INTERFACE TYPE	Phy/Wireless Phy
MAC TYPE	802.11
QUEUE TYPE	Drop tail/Priority Queue
QUEUE LENGTH	200 Packets
ANTENNA TYPE	Omni Antenna
PROPAGATION TYPE	Two ray Ground
ROUTING PROTOCOL	AODV
TRANSPORT AGENT	UDP
APPLICATION AGENT	CBR

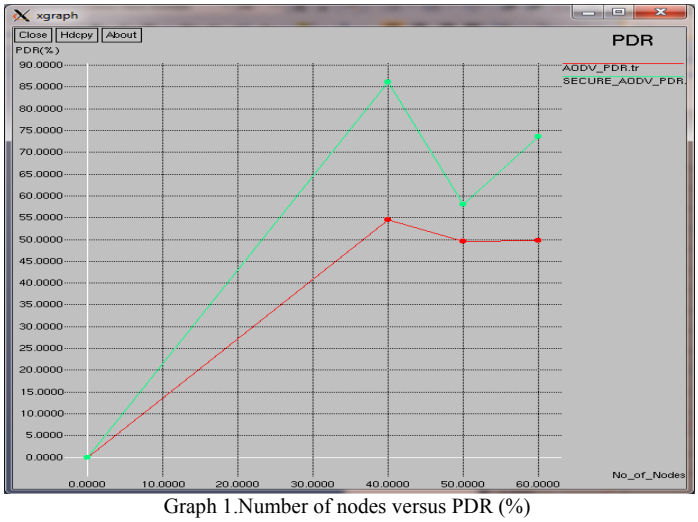
Table 1

VI. PERFORMANCE EVALUATION

Packet Delivery Ratio

- PDR is the proportion to the total amount of packets reached the receiver and amount of packet sent by source. If the amount of malicious node increases, PDR decreases. The higher mobility of nodes causes PDR to decrease.

$$PDR\ (\%) = \frac{\text{Number of packets successfully delivered to destination}}{\text{Number of packets generated by source node}}$$



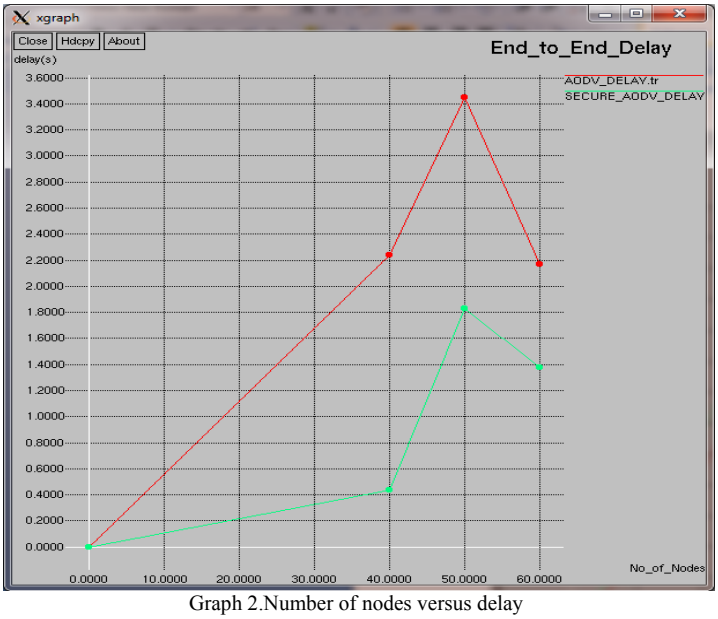
Graph 1.Number of nodes versus PDR (%)

Packet delivery ratio of SECURE_AODV is higher than that of AODV protocol. In SECURE_AODV protocol, the Impersonation attack is detected and also data will be reached at the destination is successfully. In AODV protocol the attacker drops the received packets.

End-to-End Delay

- End-to-End delay is the time taken for a packet to reach the destination from the source node.

$$\text{End to End delay (ms)} = \frac{\sum (\text{Delay of each entities data packet})}{\text{Total number of delivered data packets}}$$



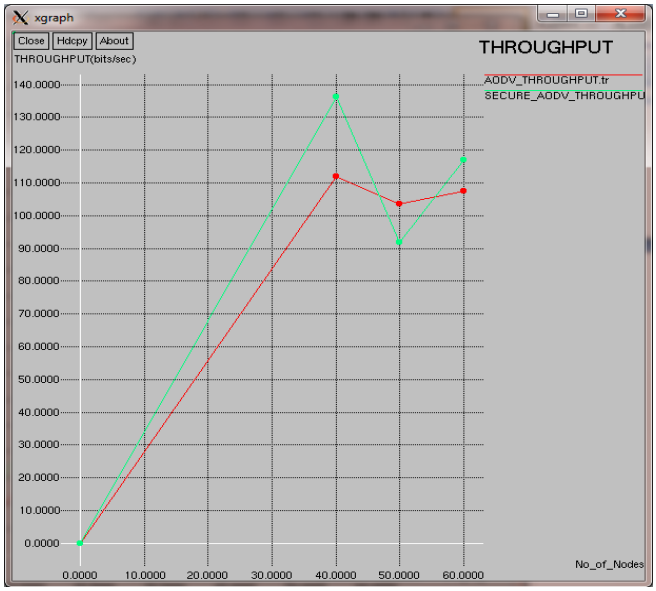
Graph 2.Number of nodes versus delay

Delay of AODV is higher than that of SECURE_AODV. In AODV protocol, many number of attacker is involved, so network traffic (congestion) is increased therefore the data reached at the destination is delayed. In SECURE_AODV, using the prevention mechanism (msg integrity and confidentiality, authentication) is to control the performance of attacker.

Throughput

- The amount of data successfully received at the destination.

  Throughput (bits/s) = Total Data / Data Transmission duration



Graph 3. Number of nodes versus throughput (bits/sec)

Throughput of SECURE_AODV is higher than that of AODV protocol. But the node is increases, in SECURE_AODV the throughput slightly degrades but after that it gets stabilized.

VII. CONCLUSION

The execution of limiting foes attains comparable comes about as those under ordinary conditions, consequently, giving solid proof of the viability of the proposed approach in catching remote mocking assaults, deciding the quantity of aggressors and restricting enemies. The proposed framework proposes hypothetical examination of utilizing the spatial association of RSS inherited from remote hubs for assault identification. It utilizes the test detail focused around the group investigation of RSS readings. An answer has likewise been given for keeping the mimic assault in the system.

References

1. Tahira Farid_ and Anitha Prahladachar Secure Routing with AODV Protocol for Mobile Ad Hoc Networks University of Windsor.
2. Preeti Bathla, Bhawna Gupta "Security Enhancements in AODV Routing Protocol" International Journal of Computer Sci ence and Technology Vol. 2,page no 295-298,june 2011
3. C. Sreedhar, Dr. S. Madhusudhana Verma, Prof. N. Kasiviswanath "A Survey on Security Issues in Wireless Ad hoc Network Routing Protocols", International Journal on Computer Science and Engineering, 02(02), 224-232(2010).
4. Michel Barbeau, Jyanthi Hall, and Evangelos Kranakis "Detecting Impersonation Attacks in Future Wireless and Mobile Networks" School of Computer Science, Carleton University, Ottawa, K1S 5B6, Canada.
5. Er. Aakansha Jain, Er. Khushboo Sawant, "Effect of Impersonation Attack on Mobile Ad Hoc Network", Indian journal of Research, 2(3), 17-19(March 2013).
6. Kimaya Sanzgiri, Bridget Dahil, Brian Neil Levine, Clay Shields, Elizabeth M. Belding-Royer, "A Secure Routing Protocol for Ad Hoc Networks"
7. Yih-Chun Hu, Adrian Perrig And David B. Johnson, "Ariadne: A Secure On-Demand Routing Protocol for Ad Hoc Networks", Springer, Wireless Networks 11, 21–38, (2005)
8. Yih-Chun Hu, Adrian Perrig And David B. Johnson, "SEAD: A Secure Efficient Ad Hoc Networks", Springer, Wireless Networks 11, (2006)
9. Kimaya Sanzgiri, Bridget Dahil, Brian Neil Levine, Clay Shields, Elizabeth M. Belding-Royer, "A Secure Routing Protocol for Ad Hoc Networks"
10. Manel Guerrero Zapata "Security In Ad Hoc Network", Universitat Politecnica de Catalunya Departament d'Arquitectura de Computadors.
11. Seung Yi "Security-Aware Ad-Hoc Routing (SAR)"
12. Latha Tamilselvan and Dr. V. Sankaranarayanan "Prevention of Impersonation Attack in Wireless Mobile Ad hoc Networks" International Journal of Computer Science and Network Security, 7(3), March 2007, 118-12

