ISSN 2395-695X (Print)
ISSN 2395-695X (Online)
International Journal of Advanced Research in Biology Engineering Science and Technology (IJARBEST)

Vol. 2, Special Issue 10, March 2016

TRUSTED THREE TIER ROUTING IN MANETS USING INTRUSION DETECTION SYSTEM

[1]P.PRITTOPAUL [2]M.USHA
[1,2]Asst.Professor, Department Of CSE,Velammal Engineering College,Chennai
p.prittopaul@gmail.com,umahalingam@gmail.com
[3]N.SAILESH KHANNA [4]A.AKASH KUMAR
[3,4] Students, Department Of CSE,Velammal Engineering College,Chennai

ABSTRACT

Today protection to networks is enhanced using many firewalls and security software's. Several of them are not adequate and effective. A Mobile Ad hoc NETwork (MANET) is a self-organized system comprised of mobile wireless nodes with peer associations. Many intrusion detection systems for Mobile Ad hoc networks are focusing on either routing protocols or their effectiveness, but they do not address the security problems. At times nodes may be selfish by not forwarding the packets to the target, thereby spiteful back the battery power. Also due to multi-hop routing and no presence of any trusted third party in open environment, MANETs are vulnerable to attacks by malicious nodes in the network. The main aim is to provide security solutions against such sort of attacks in wireless environment thus by providing confidentiality, integrity, authenticity to mobile users. This paper proposes a three-tier intrusion detection system based on trust, routing and application. The communication of data packets takes place between different nodes. First a trusted connection is established between different nodes based on few parameters. Second the routing policy is conformed for all nodes. Finally data is routed to the sink node thus by assuring authentication. The node not following trust or routing policy is considered a vulnerable node.

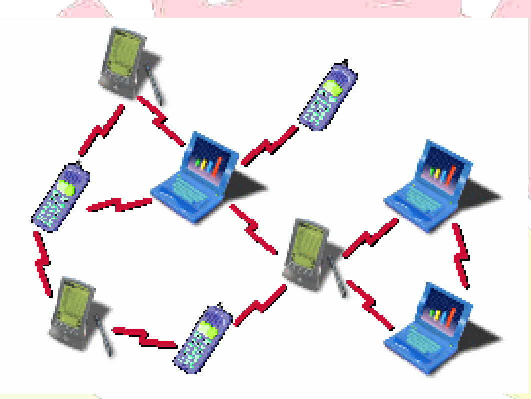
Keywords: MANET, confidentiality, authentication, intrusion detection, trust.

1. INTRODUCTION

Mobile ad hoc network is a kind of wireless network, is self-configuring infrastructures less network devices are connected by wireless. The devices of MANET network is free to move independently in any direction that's why linking with any other devices is easily done. Each must forward traffic unrelated to its own use, and therefore be a router. The primary goal of Mobile ad hoc network is each device to continuously maintain the information required to properly route traffic. Such networks may operate by themselves or may be connected to the larger Internet. The achievement of MANET is hug growth of laptops and wireless or Wi/Fi networking.

Fig.1. Mobile Ad Hoc Network

A mobile ad hoc network (MANET) as in fig.1 consists of mobile hosts equipped with wireless communication devices. The transmission of a mobile host is received by all hosts within its transmission range due to the broadcast nature of wireless communication and Omni-directional antennae. If two wireless hosts are out of their transmission ranges in the ad hoc networks, other mobile hosts located between them can forward their messages, which effectively build connected networks among the mobile hosts in the deployed area. Due to the mobility of wireless hosts, each host needs to be equipped with the capability of an autonomous system, or a routing function without any statically established infrastructure or centralized administration. The mobile hosts can move arbitrarily and can be turned on or off without notifying other hosts. The mobility and autonomy introduces a dynamic topology of the networks not only because end hosts are transient but also because intermediate hosts on a communication path are transient.



1.1 TYPES OF ATTACKS

1) Flooding Attack

Flooding is a type of Denial of Service (DoS) attack in MANET. Intentional flooding may lead to disturbances in the networking operation. This kind of attack consumes battery power, storage space and bandwidth. Flooding the excessive number of packets may degrade the performance of the network.

2) Black Hole Attack

The black hole problem is one of the security attacks that occur in mobile ad hoc networks (MANETs). We present two possible solutions. The first is to find more than one route to the destination. The second is to exploit the packet sequence number included in any packet header.

3) Link Spoofing Attack

In a link spoofing attack, a malicious node advertises fake links with non-neighbors to disrupt routing operations. For example, in the OLSR protocol, an attacker can advertise a fake link with a target's two-hop neighbors. This causes the target node to select the malicious node to be its MPR. As an MPR node, a malicious node can then manipulate data or routing traffic, for example, modifying or dropping the routing traffic or performing other types of DoS attacks.

4) Worm Hole Attack

A wormhole attack is a particularly severe attack on MANET routing where two attackers connected by a high-speed off-channel link called the wormhole link. The wormhole link can be established by using a network cable and any form of wired link technology or a long-range wireless transmission in a different band.

5) Colluding mis-relay Attack

In colluding misrelay attack, multiple attackers work in collusion to modify or drop routing packets to disrupt routing operation in a MANET. This attack is difficult to detect by using the conventional methods such as watchdog and path rater.

6) Denial of Service Attack

In computing, a denial-of-service (DoS) or distributed denial-of-service (DDoS) attack is an attempt to make a machine or network resource unavailable to its intended users. A DoS attack generally consists of efforts to temporarily or indefinitely interrupt or suspend services of a host connected to the Internet.

2 .LITERATURE SURVEY

1 A. Akhtaret. al. has presented —Energy Aware Intra Cluster Routing for Wireless sensor networks, in 2010. A new technique for intra cluster routing which is more energy efficient than a well-known routing protocol Multihop Router that performs multihop routing is proposed [1]. They proved their idea by simulating a network of 30 nodes in TOSSIM. While justifying the idea through results of the simulation had been considered the parameters that include: number of packets sent in the network, energy consumed by the network, remaining energy level of nodes at specific time and network lifetime of the network. By using proposed technique shows that they had increased the network lifetime and number of packet sent in the network.

2 Zijian Wang et. al. has presented —Energy Efficient Collision Aware Multipath Routing for Wireless sensor networks, in 2009. An energy efficient and collision aware (EECA) node-disjoint multipath routing algorithm has been proposed [2]. The main idea of EECA is to use the broadcast nature of wireless communication to avoid collisions between two discovered routes without extra overhead. Additionally, EECA restricts the route discovery flooding and adjusts node transmit power with the aid of node position information, resulting in energy efficiency and good performance of communication. They used NS-2.33 simulator to evaluate the proposed scheme in terms of the average packet delivery ratio, the average end-to-end delay, the average residual energy and the number of nodes alive. Their preliminary simulation results show that ECCA algorithm results in good overall performance, saving energy and transferring data efficiently.

3 Lu Su et. al. has presented —Routing in Intermittently Connected sensor networks, in 2009. Identifies the challenges of routing in intermittently connected sensor networks and proposed [4] an on demand minimum latency routing algorithm (ODML) to find minimum latency (ODML) to find minimum latency routes. They proposed two proactive minimum latency routing algorithms: optimal PML and quick—PML. The schemes proposed in this paper can provide generic routing functionalities for most of the existing scheduling schemes.

4 A.P.Subramanianet. al. has presented —Multipath Power Sensitive Routing Protocol for Mobile Ad hoc Networks, in 2004. The Multipath Power Sensitive Routing (MPSR) Protocol[7] for Mobile Ad hoc Networks has been presented. Providing multiple paths is useful in ad hoc networks because when one of the routes is disconnected, the source can simply use other available routes without performing the route discovery process again. The simulation was done using the Global Mobile Simulator (GloMoSim) Library. The results of extensive simulation show that the performance of MPSR protocol is on an increasing trend as mobility increases when compared to the Dynamic Source Routing and using this protocol is that the end-to-end packet delay does not increase significantly.

5 Fan Ye et. al. has presented —A Two-Tier Data Dissemination Model for Large-scale Wireless sensor networks, in 2002. TTDD, a two-tier data dissemination design [9], to enable efficient data dissemination in large-scale wireless sensor networks with sink mobility has been described. Instead of passively waiting for queries from sinks, TTDD exploits the property of sensor being stationary and location-aware to let each data source build and maintain a grid structure in an efficient way. Queries are forwarded upstream to data sources along specific grid branches, pulling sensing data downstream toward each sink. They implement the TTDD protocol in ns-2 and used the basic greedy geographical forwarding with local flooding to bypass dead ends. Their analysis and extensive simulations have confirmed the effectiveness and efficiency of the proposed design, demonstrating the feasibility and benefits of building an infrastructure in stationary sensor networks.

6 Sameer Tilaket. al. has presented "A Taxonomy of Wireless Micro-sensor Network Models, in 2002. Emerging field to classify wireless micro-sensor networks [11] according to different communication functions, data delivery models, and network dynamics is examined. This taxonomy will aid in defining appropriate communication infrastructures for different sensor network application subspaces, allowing network designers to choose the protocol architecture that best matches the goals of

their application. In addition, this taxonomy will enable new sensor network models to be defined for use in further research in this area.

7 M. Youniset. al. has presented —Energy-Aware Routing in Cluster-Based sensor networks, in 2002. A novel energy-aware routing approach for sensor networks [13] is introduced. A gateway node acts as a cluster-based centralized network manager that sets routes for sensor data, monitors latency throughout the cluster, and arbitrates medium access among sensor. The gateway configures the sensor and the network to operate efficiently in order to extend the life of the network. Simulation results demonstrate that the algorithm consistently performs well with respect to both energy-based metrics, e.g. network lifetime, as well as contemporary metrics, e.g. throughput and end-to-end delay.

8 C. Schurgerset. al. has presented —Energy Efficient Routing in Wireless sensor networks, in 2002. Argument betweenoptimal routing in sensor networks is infeasible and proposed a practical guideline that advocates a uniform resource utilization, which can be visualized by the energy histogram is presented. They also propose a number of practical algorithms that are inspired by this concept. Their DCE combining scheme reduces the overall energy [14], while their spreading approaches aim at distributing the traffic in a more balanced way. Several techniques, which rely only on localized metrics, are proposed and evaluated. This result shows that they can increase the network lifetime up to an extra 90% beyond the gains of our first approach.

9 Curt Schurgerset. al. has presented —Energy Efficient Routing in Wireless sensor networks, in 2001. Argument on optimal routing in sensor networks [15] is infeasible and proposed a practical guideline that advocates a uniform resource utilization, which can be visualized by the energy histogram is presented. They proposed a number of practical algorithms that are inspired by this concept. There DCE (Data Combining Entities) combining scheme reduces the overall energy, while there spreading approaches aim at distributing the traffic in a more balanced way. Several techniques, which rely only on localized metrics, are proposed and evaluated. And there result shows that they can increase the network lifetime up to an extra 90% beyond the gains of their first.

3. TRUSTED THREE –TIER MODULE

In fig.3.1, the source contains the data to be sent to the destination in a secured way. So the data has to be sent through a path that has no intruders, therefore the data is being collected and sent to the node that is right next to the source. The IDS detects if there are any intruders in the path, if there is any intruder the node reports it to the source and takes an alternative path to reach the destination. The destination then sends the secure acknowledgement on receiving the data to the source node to enhance secure communication.

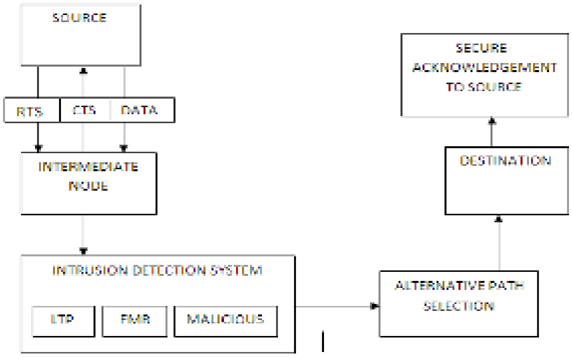

SOURCE
RTS
CTS
DATA
INTERMEDIATE NODE
INTRUSION DETECTION SYSTEM
LTP
FMR
MALICIOUS
ALTERNATIVE PATH SELECTION
DESTINATION
SECURE ACKNOWLEDGEMENT TO SOURCE

Fig 3.1Architecture Diagram

3.1 Node creation and Data Forwarding:

Nodes are created to form a mobile network. The nodes send messages to communicate its presence in the network. Request to Send (RTS) is sent by the source to the intermediate nodes and the intermediate nodes send Clear to Send (CTS) as a reply. After the assurance is made between the nodes, the data is forwarded. ACK (Acknowledgement) is sent in response to the data packet received.

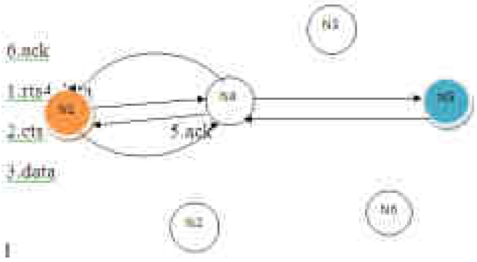


Fig. 3.2 Data forwarding and Acknowledgement

- Initially the source node N1 sends the RTS (request to send) message to node N4.
- Node N4 sends a CTS(clear to send) message as a reply
- Only then the link is established and N1 sends data to N4.
- Now N4 forwards the data to N5 following the route discovery phase of DSR protocol.
- Node N5 being the destination receives the data and sends back the acknowledgement to N4.
- N4 forwards acknowledgement to the source along with the information regarding the path that the data has travelled (N1, N4, and N5).

3.2 INTRUSION DETECTION SYSTEM

In a network or a system, any kind of unauthorized or unapproved activities are called intrusions. An Intrusion Detection System (IDS) is a collection of the tools, methods, and resources to help identify, assess, and report intrusions. Intrusion detection is typically one part of an overall protection system. These local IDSs trigger the global IDS which necessitate collaborative decision of the nodes neighboring the flagged node. This decision is made through a majority voting process.The intruder in the path along which the data is transmitted from source to destination (i.e.). Malicious node is identified and an alternative path is taken up by the source node.
Intrusions in a network may happen in various ways:

- **Attempted break-in:**An attempt to have an unauthorized access to the network.
- **Masquerade:** An attacker uses a fake identity to gain unauthorized access to the network.
- **Penetration:**The acquisition of unauthorized access to the network.
- **Leakage:**An undesirable information flow from the network.
- **DoS:** Blockage of the network resources to the other users**.**
- **Malicious use:**Deliberately harming the network resources. IDSs may provide partial detection solution to those attacks.
- **Interval Rule:**delay between the arrivals of two consecutive messages must be within certain limits. Retransmission rule: the transit messages should be forwarded by the intermediate nodes.
- **Integrity Rule:**the original message from the sender must not deviate when it arrives to the receiver.
- **Delay rule:** the retransmission of a message must occur after a certain wait time.
- **Repetition Rule:**Same message can only be transmitted from the same node in certain number of counts.

- **Jamming Rule:**The number of collisions for a packet transmission must be lower than a threshold.
- **Low Transmission Power:** Packet is lost due the low transmission power of the node.

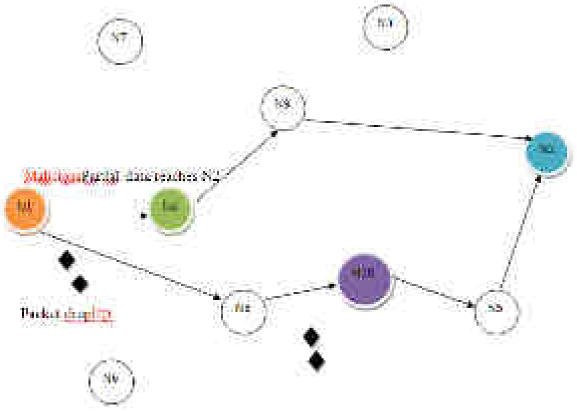


Fig. 3.3. Identification of Malicious and LTP nodes

- Node N1 is the source and it sends data to N4.
- Loss of data occurs due to the malicious behavior of N4.
- N4 forwards the data that it has received to N9 and N9 forwards the data to the destination N2.
- But the data is only partial data due to the data loss caused by N4.
- The data is then transmitted along another path i.e. via N8.
- Node N8 has low transmission power and thus it does not transmit the entire data sent by the source.
- Data loss occurs yet data is forwarded to N10.
- N5 receives data from N10 and forwards it to the destination N2.
- Thus data loss exists in this path also.
- The presence of these intruders is informed to the source along with the acknowledgement sent to the source.
- The source keeps track of the intruders along different paths.
- The path that does not have malfunctioning nodes is chosen to send data.
- If two or more paths exist, the shortest among them is chosen as the best path.

3.3 SECURE INTRUSION DETECTION SYSTEM:

Members of the network are not aware of the intrusions happening around them because stand-alone IDS do not allow individual nodes to cooperate or share information among each other. They work as if they are alone. This is proposed for flat network infrastructures. Each node runs an IDS agent which participates in the intrusion detection and response of the overall network. If a node detects an intrusion with weak or inconclusive evidence, then it can initiate cooperative global intrusion detection procedure for secure communication. If a node detects an intrusion locally with sufficient evidence, then it can independently alert the network regarding an attack and send the data through another alternative node. Similarly the acknowledgement is also sent along the same path. But the number of nodes along the path increases. So clusters are formed and the cluster heads are chosen and the intruders in each cluster are known to the cluster head. The data is now sent along the shortest path possible.

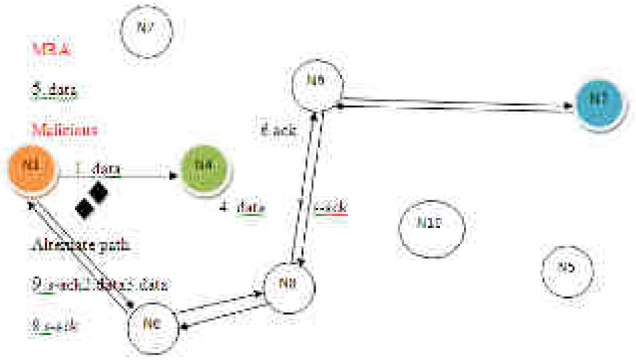
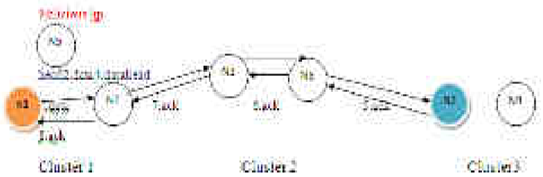


Fig 3.4 Misbehaviour Report Authentication and Secure Ack.

- Source node forwards data to node N4, there is packet drop and thus N4 is marked as malicious.
- So N1 takes an alternative path and forwards data to N6.
- N6 receives the data and being the intermediate node it forwards the data packet to the next nearest node.
- N8 receives data and forwards it to N9 which then forwards the data to N2 i.e.the destination node without any loss of data.
- The destination N2 sends the acknowledgement to N9 along with route information.
- Misbehavior Report Authentication is done by N9 and thus it does not forward the acknowledgement via. N4 (Malicious).
- The Secure Acknowledgement(s-ask) is forwarded by N9 to N8 and then N8 forwards it to N6.
- Finally the acknowledgement reaches the source without any loss.



.Fig 3.5 Cluster formation and Data forwarding

- However the number of intermediate nodes to the destination increases.
- So we go in for formation of clusters and then transmit data from source to destination.
- The nodes in the network group together into clusters by sending cluster request message to a node.
- The cluster is thus formed with a cluster head which broadcasts a data and identifies the intruders within the cluster and shares this information with other members of the cluster so that they do not forward data to these intruders.
- The data is not forwarded to the intruders in order to avoid the data packet loss.
- Here in the above figure node N1 is the source and it forwards the data to N7 belonging to the same cluster.
- N7 forwards the data to N3 belonging to Cluster 2.
- From N8 data is forwarded to N8 and then finally to the destination N2.
- The destination then responds with an acknowledgement which reaches the source N1 via N8-N3-N7.

The number of intermediate nodes is comparatively less and there is no loss of data as the data is not forwarded to the intruders.

4. EXPERIMENTAL ANALYSIS

To evaluate the performance of the proposed system, we use the ns2 discrete event simulator. Simulation results shown here for delay ratio, Total Losses and Throughput Workload Compared with Existing System.

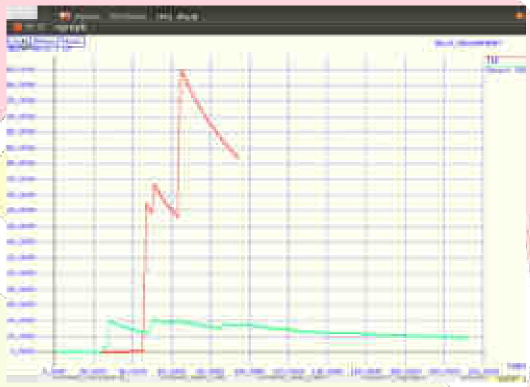


Fig 4.1 Delay Ratio

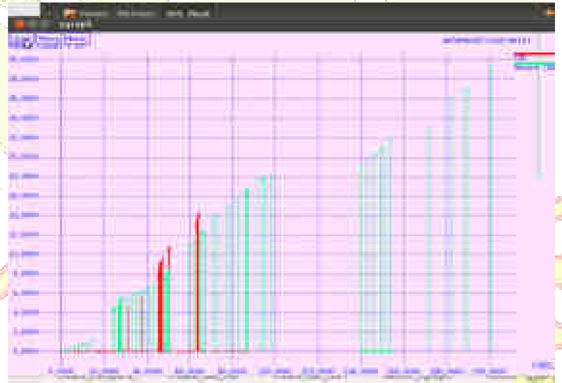
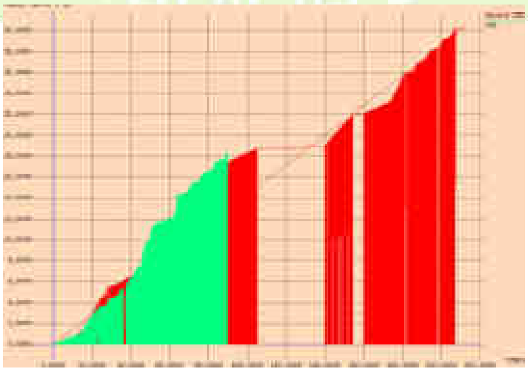


Fig. 4.1 .Total Losses.



.

Fig. 4.3 .Throughput Workload

CONCLUSION

In this paper we have the analysis in terms of delay ratio and ratio of packet loss that gets decreased when compared to the existing system. The three tier architecture provides security and authentication between nodes which leads to secure communication over network.

REFERENCE

[1] A. Akhtar, ”Energy Aware Intra Cluster Routing for Wireless sensor networks”, vol. 3, pg. 29, 2010.

[2] Zijian Wang, ”Energy Efficient Collision Aware Multipath Routing for Wireless sensor networks”, vol. 1, pg. 1-5, 2009.

[3] Ming Liu, ”An Energy-Aware Routing Protocol in Wireless sensor networks”, vol. 3, pg. 445-462, 2009.

[4] Lu Su, ”Routing in Intermittently Connected sensor networks”, vol. 2, pg. 278-287, 2009.

[5] A.P.Subramanian, ”Multipath Power Sensitive Routing Protocol for Mobile Ad hoc Networks”, vol. 1, pg. 1-5, 2004.

[6] Fan ye, ”A Two-Tier Data Dissemination Model for Large-scale Wireless sensor networks”, vol. 3, pg. 148-159, 2002.

[7] Sameer Tilak, “A Taxonomy of Wireless Micro-sensor Network Models”, vol. 6, pg. 460-470, 2002.

[8] M. Younis, ”Energy-Aware Routing in Cluster-Based sensor networks”, vol. 2, pg. 129-136, 2002.

[8] C. Schurgers, ”Energy Efficient Routing in Wireless sensor networks”, vol. 1, pg. 131-141, 2002.

[10] Curt Schurgers, ”Energy Efficient Routing in Wireless sensor networks”, vol. 1, pg. 357-361, 2001.

[11] Fuchsberger, “Intrusion detection systems and intrusion prevention systems”, Elsevier J. Information Security Technical Report, vol. 10, pg. 134-139, 2005.

[12] M. Ngadi, A.H. Abdullah, and S. Mandala, “A survey on MANET intrusion detection”, International J.Computer Science and Security, vol. 2, pg. 1-11, 2008.

[13] Y. Zhang, W. Lee, and Y.A. Huang, “Intrusion detection techniques for mobile wireless networks”, J. Wireless Networks, vol. 9, pg. 545-556, 2003.

[14] E. Cayirci and C. Rong, “Security in Wireless Ad Hoc and Sensor Networks”, book published by Wiley,vol. 6,pg 460-470, 2009.