International Journal of Engineering Research and Development
e-ISSN: 2278-067X, p-ISSN: 2278-800X, www.ijerd.com
Volume 10, Issue 11 (November 2014), PP.64-69

A Survey on Securing TORA for Detecting and Protecting Against Sybil Attack in MANETs

Suraj Thawani[1], Hardik Upadhyay[2]
[1]*GTU PG School, Research Scholar, Ahmedabad, India.*
[2]*GPERI, Assistant Professor, Ahmedabad, India.*

Abstract:- Mobile Ad-hoc Network (MANET) is a quite challenging to ensures security because if it's open nature, lack of infrastructure, and high mobility of nodes. MANETs is a fast changing network in a form of decentralized wireless system. It requires a unique, distinct and persistent identity per node in order to provide their security and also has become an indivisible part for communication for mobile device. In this phase of dissertation, we have focused giving security to Temporally Ordered Routing Protocol Algorithm (TORA) from Sybil attack. TORA is based on a family of link reversal algorithm. It is highly adaptive distributing routing algorithm used in MANET that is able to provide multiple loop-free routes to any destination using the Route Creation, Route Maintenance and Route Erasure functions. Sybil attack is a serious threat for wireless networks. This type of attacker comes in the network and they start creating multiple identities. From that multiple identities they are disrupting the network by participating in communication with line breaking nodes. This cause's huge loss in network resources. These networks can be protected using network failure and firewall detection schemes for detecting the attack and minimizing their effects. Proposed approach is expected to secure TORA through the implementation. Performance factor of network would be taken into consideration in order to verify the efficiency of modified TORA in MANET environment.

Keywords: - Mobile Ad-hoc Networks, TORA, Security, Sybil Attack.

I. INTRODUCTION

A mobile ad-hoc network (MANET) is a non-aligned system of mobile routers and hosts connected by wireless links [1]. These nodes includes laptop, computer and wireless phones etc., have a limited conveyance range. The routers are free to move randomly because it is a self-configuring infrastructure less network of mobile device connected by wireless. Thus, the network is wireless topology that may change rapidly and randomly. These networks are erect, work and maintained by its own because each node performs two role, one for router and one for host. In MANET, each node search for the support of its neighbouring nodes to forward packets in a peer-to-peer fashion with no cluster architecture. Because of this, most of protocol except that other nodes are trustable reliable, so they do not consider the security and attack issues. In this, it is hard to determine which node has really leaved the network, location changed or it has been blocked or intercepted.

A. MANET challenges [1]

1) Power Awareness:
In MANET, the node are run on batteries so there are limited power for processing.

2) Dynamic Topology:
In this, the network is self-organizing because nodes are mobile. Thus, the network keeps changing ever time in the topology.

3) Quality of Service:
In environment, the constant QoS for different multimedia services is frequently changing.

4) Multicast Routing:
In multicast routing protocol, it is constantly changing the MANET environment.

5) Security:
Security is extremely important in scenarios such as a theatre. Security has main goals that are – availability, confidentiality and integrity.

B. Classification of Routing Protocols in MANETs

Routing protocols for mobile ad-hoc networks (MANETs) can be broadly classified into Reactive (on-demand) routing protocol, Proactive routing protocol and Hybrid protocols. A routing protocol are used to discover routing path between all the nodes [2].

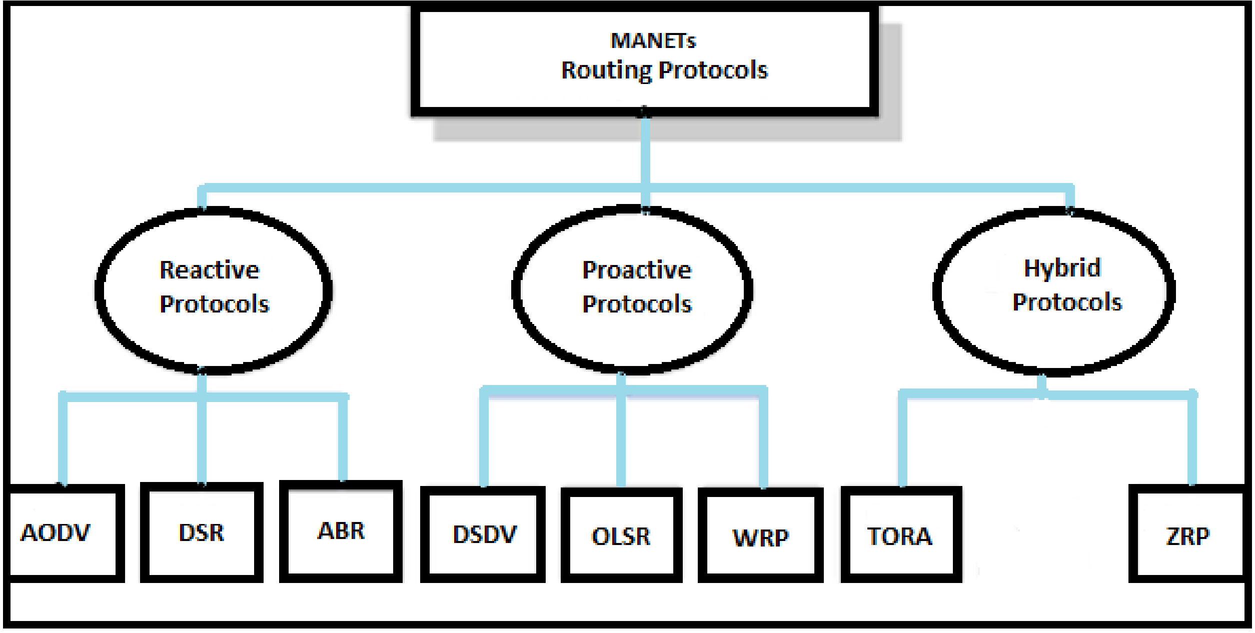

Figure 1: MANETs Routing Protocols

In proactive routing protocol every node in the network has one or more routes to any possible destination in its routing table at any given time. Proactive routing protocols includes Optimized Link State Routing (OLSR), Destination Sequence Distance Vector (DSDV) and there are also other protocols like Wireless Routing Protocol (WRP). Its main advantage is that it gives regular updates of data traffic.

In reactive routing protocol every node in the network obtains a route to a destination on a demand fashion. Reactive protocols do not maintain up-to-date routes to any destination in the network and do not generally exchange any periodic control messages. In this reactive routing protocol includes Ad-hoc On Demand Distance Vector (AODV) routing and Dynamic Source Routing (DSR).

In hybrid routing protocol every node acts reactively in the region close to its proximity and proactively outside of that region or zone. In this hybrid routing protocol includes Temporarily Ordered Routing Protocols (TORA) and Zone Routing Protocol (ZRP).

C. Types of Attack in MANETs [8]

The security attacks in MANET can be classified into two major categories, i.e.; internal attacks and external attacks.

-Internal Attacks:

In this type of attack, it initiated by the authorized node in the networks. It direct attacks on the node in the specific working network. This type of attack broadcast the wrong information to the other nodes, then that can be a misbehaving node or compromised node.

-External Attacks:

In this type of attack, it initiated from outside source, it doesn’t belong to the network. The attacker attempts to cause network congestion, denying access to the specific network, or destroy the whole networks.

Many possible attacks in MANET that can be compromise the security of TORA in mobile ad-hoc networks. They are

1) Impersonation:

This type of attacker can act as an original node and join the network, then after they control the full network and conduct malicious behaviour. They spread fake routing information and they collect the secret information from the nodes. If network doesn’t keep the proper authentication mechanism then it is vulnerable to the networks.

2) Denial of Service:

In denial of service, attacker first checks the specific node, if the node is not in the service then it attacks in the entire network. So this type of attack may disturb the entire service of network.

3) Eavesdropping:

In this type of attack, the main goal of the attacker is to get some private information. Then it is being transferred from one node to the other. This attack is very much complex, which finds the secret information of the nodes and get compromised due to this attack.

4) Black Hole Attack:

In this, opponent traps the traffic at the main centre of the network close to a compromised. In this type of attack, attacker offers an attractive path to the neighbouring nodes. A black hole attack is also paired with other attacks like packets dropping, denial of service and etc.

5) Wormhole Attack:

In this, opponent connects two distant parts of the network and convey messages received in different part of the network to the other. A lower latency link is used to pass the messages in this type of network.

6) Sybil Attack:

In this type of an attack, a particular node in the network makes a several different fake identities to get the specific information about the network. Because of the malicious attack there is great decrease in the multipath topology in routing, distributed storage, maintenance etc.

II. TEMPORALLY ORDERED ROUTING PROTOCOL ALGORITHM (TORA)

The author Park et.al. Presents TORA. Temporally Ordered Routing Protocol Algorithm (TORA) is a highly modified, scalable and efficient distributed routing algorithm based on the concept of link reversal [4]. It uses mixture of reactive and proactive routing. TORA is able to provide multi-hop wireless network, which routes freely to any destination originated on-demand routing protocol by modelling the entire network as a Directed Acyclic Graph (DAG). Each nodes of links flow from higher height to lower height which is associated with height [5]. All the nodes will route to the destination. DAG is separately constructed for each destination. In TORA, links between nodes are bi-directional, nodes are always aware of their neighbouring nodes. Packets are received reliably in the correct order and then broadcasting is used. TORA has the main feature that very small set of nodes are localized by control messages near the instance of topological change. Through the routing information, nodes need to maintain the adjacent nodes. It has three basic functions [7]:

-Route Creation
-Route Maintenance
-Route Erasure

A. Route Creation:

In route creation, all nodes start off with null height and links between the nodes are unassigned. It initiates route creation when a node requires a route to a destination. A QRY (query) packet contains the destination id of the node and the reply to the query is called update (UPD) packet. When a node get the notification from the receiver as an update packet, then it makes the direct link to the sender. From this link, route required is set, whenever packet wants to send the message it will directly send the message because route is set to the destination. If link is break then it rebroadcast the query to find the node and sends the message.

B. Route Maintenance:

In route maintenance, it occurs only when all outgoing links breaks from the node which routes to a destination. The detection of a link failure or link reversal can be affect by the update packet. When a node loses its entire outgoing links through the detection of link failure then the node propagates an update packet which reverses the links to all of its neighbouring node. When the nodes receive an update packet then it reverses the links to their neighbouring nodes. In this route maintenance, links are reversed only for neighbouring nodes. They do not have any out-going links and not performed any link reversal recently. Links are reversal repeated till each of the node has at least one out-going link. In this process it ensures that the directed acyclic graph is maintained to all nodes that routes at the destination. In route maintenance function of TORA, it has the main problem that it produces a large amount of routing overhead. Because of large amount of routing overhead it causes the network to reach the destinations. In route maintenance, our aim is to restrict the large amount of data packet which are continues participating in data communication. From restricting the large amount data packet in the network, it reduces routing overhead and allowing them for delivery of data packets.

C. Route Erasure:

In route erasure, the packets are automatically clears because the node is participating in the network without a route to the destination. Because of link failure in route maintenance, the nodes are undertaken to check all of its out-going links. During the route maintenance, the update packet are sent by the node to reverse the links of all its neighbouring nodes. In the maintenance, network do the partition in the nodes to find out the route to the destination. If update packet is send back by another node then that node is route to the destination. And, if the node is not found in the partition part of network then the route erasure is performed. Route erasure clear packets in the network and its neighbour's links are unassigned. Through the clear packets all the routes are erase in the network which are unreachable to the destination.

Advantages:

- In TORA multiple routes are supported between sources to destination. If the node fails or removes that node is quickly resolved without source involvement by switching to an alternate route to improve blockage.
- In TORA communication overhead and bandwidth utilization is minimized because it does not require a periodic update.
- Link status sensing and neighbour delivery, dependable, order packet delivery and security authentication are the support of TORA.

Disadvantages:

- In ad-hoc network, nodes are depended on the synchronized clocks.
- The link status sensing, neighbour discovery, order packet delivery and address resolution are used to run IMEP (Internet MANET Encapsulation Protocol) on the intermediate lower layer below the TORA.
- It's difficult to separate from the lower layer because this has makes the protocol overhead.

Characteristics:

- Distributed
- Loop-free routing
- Multi-path routing
- Minimization of communication overhead via localization of algorithmic reaction to topological changes

III. SYBIL ATTACK

The author Gong Jun Yan et.al. Presents Sybil attack. In present, Sybil attack is the serious threat in ad-hoc networks. In Sybil attack, attacker makes the multiple identities in the network as a malicious node with the several address. Each nodes in the network has given unique address. It make fake identities in the network to collect the private information from the nodes. It only occurs when one node is connected to other node to breaks the link and collects the information from the nodes. This type of attack behaves like an original node as a malicious node and it affect the network because it makes infinite number of fake identities on one physical device. Because of fake identities it harms the environment and damages the many application in the network [3].

A. Three taxonomies for Sybil Attack [9]:

1) Direct and Indirect Communication:

In the direct communication, the Sybil node and the authentic node communicate with each other directly. This means, when authentic node sends the message to the Sybil node then malicious node listen to this node. When any message sent from the Sybil node it is actually from the malicious node device to collect the particular information the network. In this direct validation, it test the node directly whether the other node is valid or not.

In the indirect communication, Sybil node is not communicating directly with the authentication node they actually communicate with one or more malicious node to reach the Sybil node at the destination. In this indirect validation, in which nodes that have already been verified are allowed as invalidate for other nodes.

2) Fabricated and Stolen Identities:

In Sybil node, there are two different ways to get the identity. It can be fabricated identity or it can steal an identity from one of the authentic nodes.

In *fabricated identities*, if there is no restricted identity or some way to verify that an identity is authentic, then malicious node simply identify random node and join the network.

In *stolen identities*, if there is possibilities of joining the network through the fake identities, then the attacker try to assign authentic identities to the Sybil nodes. Then this identity theft may be ignored through the disabling the fraud nodes.

3) Simultaneity:

In simultaneous attack, the attacker tries to participate all the Sybil nodes in the network once at the same time.

In non-simultaneous attack, the attacker tries to participate all the Sybil nodes in the network, but at the given time only several identities can participate in network. The attacker detects the identity, which identity is going and which one is entering in the network.

In Sybil attack, it is serious impact of detecting the Sybil attack in network and protect the network from the attackers.

B. Forms of Sybil Attacks [6]:

1) Routing:

In ad-hoc network, Sybil attack can disrupt the routing protocol by participating in network, especially in location-based or multipath routing mechanism. This multipath routing attacks as a single attacker, but there is also another routing protocol which makes more than one identity of malicious node at same places and at same time i.e.; geographical routing.

2) Distributed Storage:

In this type of attack, it makes multiple identities of node on the network to collect the data from the system. It uses peer-to-peer communication, in which malicious node behaves as an original node to collect the data from the file storage system

3) Data Aggregation:

A few network protocol use the same value of data aggregate instant of other value in network. It harms the reading of aggregation by using the same aggregation value.

4) Fair-Resource Allocation:

In this type of attack, it shares the unfair resource to the nodes from malicious nodes through different identities in the network. While sharing the resource through the malicious node is attack to the nodes.

5) Voting:

In this environment, when the voting scheme is place for reporting or identifying the node, it make several node of multiple identities in the network. Sybil attack is done by making multiple identities for voting in this system.

IV. COUNTERMEASURES AGAINST SYBIL ATTACK

Sybil attack is the fundamental problem in many systems. In a wired context, peer-to-peer applications is done. Away from the attacker, detection and protection is done below [9]:

A. Trusted Certification:

In the trusted certification, it is common solution due to its potential to completely remove Sybil attacks. In this each node has its own identity through which it indicates guarantees the certificate. There is no method for ensuring uniqueness, it is performed by manual configuration. This configuration can be costly and there is large-scale of restriction in systems. But it guarantees the existence to detect and protect against the fake identities which are stolen or lost. It is difficult to implement in ad-hoc networks because it requires lack of infrastructure.

B. Trusted Devices:

This device combined with the trusted certifications to make one hardware device in one network entity. There is main issue that from multiple hardware device it cannot prevent one entity, it can only make one entity in network through manual intervention.

C. Domain Specific:

In domain specific, there are some countermeasures that are applications. For example, detection of each node is based on the location in the mobile ad-hoc networks. In the Sybil attack, all the identities move together with single device. In mobile networks there is no defense applicable.

D. Resource Testing:

In resource testing, there is limited bandwidth for each physical entity of a resource. All the resources of identities are independent with each other. In this verifier tests the identities, that all the physical entities are different with the independent physical device. This checks computing power, storage ability and network bandwidth. This technique is done by SybilGaurd, which relies limited availability of nodes.

E. Recurring Costs and Fees:

In this technique, testing is done in the limited number of Sybil nodes and given a time of period. In Sybil attack, charging a fee for each identity is more effective but one time fees suffer only a constant cost.

F. Computational Resource Testing:

In this testing, nodes in the network uses limited computational power. Nodes have a limit power on the number of crypto-puzzles at the time period. This crypto-puzzles is solved by the cryptographic problem by the calculation in the certain amount of time.

G. Radio Resource Testing:

In this radio resource testing, nodes only possess one radio device with the limitation of devices. Take the example of limitation, that incapability of a radio simultaneously transmitting in two different frequencies.

V. CONCLUSIONS

Mobile Ad hoc Networks (MANETs) have received growing research attention in recent years. Mobile ad hoc networks are wireless networks that use multi-hop routing alternatively of constant networks base to provide network connectivity. The work is done towards to securing TORA in MANET. Temporarily Ordered Routing Protocol (TORA) is a distributed routing algorithm that is based on a family of link reversal algorithms. Sybil attack is an injurious attack in MANETs, attacker makes the multiple identities in the network as a malicious node with the several address. Each nodes in the network has given unique address. It make fake identities in the network to collect the private information from the nodes. The method to detect and protect against Sybil attack is testing the resource certificate authority.

REFERENCES

[1]. H. Ehsan, F. A. Khan, "Malicious AODV: Implementation and Analysis of Routing Attacks in MANETs", IEEE 11th International Conference on Trust, Security and Privacy in Computing and Communications, 2012.

[2]. Rajeswari M., Dr. P. U. Maheswairi, Bhuvaneshwari S., Gowri S., "Performance analysis of AODV, DSR, TORA and OLSR to achieve group communication in MANET", IEEE 4th International Conference on Advanced Computing, December 2012.

[3]. S. Abbas, M. Merabti, D. Llewellyn-Jones, K. Kifayat "Lightweight Sybil Attack Detection in MANETs" IEEE System Journal, June 2013.

[4]. A. K. Gupta, Dr. H. Sadawarti, Dr. A. K. Verma "Performance analysis of AODV, DSR & TORA Routing Protocols" IACSIT International Journal of Engineering and Technology, April 2010.

[5]. K. H. Lim and A. Datta "An In-depth Analysis of the Effects of IMEP on TORA Protocol" IEEE Wireless Communications and Networking Conference: Mobile and Wireless Networks, 2012.

[6]. Sowmya P., V. Anitha "Defence Mechanism for Sybil Attacks in MANETS using ABR Protocol" International Journal of Advanced Computer Research, June-2014.

[7]. K. H. Lim and A. Datta "Enhancing the TORA Protocol using Network Localization and Selective Node Participation" IEEE 23rd International Symposium on Personal Indoor and Mobile Radio Communication (PIMRC), 2012.

[8]. M. Pandya, A. Shrivastava and R. Gandhi "Improvising the Performance with Security of AODV Routing Protocol in MANETs" Nirma University International Conference on Engineering (NUiCONE), 2013.

[9]. D. Monica "Thwarting the Sybil Attack in Wireless Ad-hoc Networks" INSTITUTO SUPERIOR TECNICO (IST), July 2009.