International Journal of Computing and Business Research (IJCBR)

ISSN (Online) : 2229-6166

Volume 4 Issue 3 September 2013

SURVEY OF CHALLENGES AND SOLUTIONS IN MANET

Er. Sukhvir Boora
Asst. Prof. in Dept. of CSE, ,
NCCE, Israna,

Er. Shayog Sharma
Research Scholar
NCCE Israna

Dr. Sima
Asst. Prof. in Dept of C.S.E.
KITM, Karnal

Abstract: In this paper the authors present a survey of secure ad hoc routing protocols for wireless networks. Ad hoc network is a collection of nodes that is connected through a wireless medium forming rapidly changing topologies. Attacks on ad hoc network routing protocols disrupt network performance and reliability with their solution. They briefly present the most popular protocols that follow the table-driven and the source-initiated on-demand approaches. The comparison between the proposed solutions and parameters of ad hoc network shows the performance according to secure protocols. The authors discuss in this paper routing protocol and challenges and also discuss authentication in ad hoc network

Keywords: Security, Ad hoc Networks, Routing Protocols, Key Management.

1. INTRODUCTION TO MANET

Ad-hoc networks are a new paradigm of wireless communication for mobile hosts. No fixed infrastructure such as base stations as mobile switching .Nodes within each other radio range communicate directly via wireless links while these which are far apart rely on other nodes to relay messages. Node mobility causes frequent changes in topology.

2. CHALLENGES OF MANET

The salient features of ad hoc networks pose both challenges and opportunities in achieving these security goals. First, use of wireless links renders an ad hoc network susceptible to link attacks ranging from passive eavesdropping to active impersonation, message replay, and message distortion. Eavesdropping might give an adversary access to secret information, violating confidentiality. Active attacks might allow the adversary to delete messages, to inject erroneous messages, to modify messages, and to impersonate a node, thus violating availability, integrity, authentication, and non-repudiation. Secondly, nodes, roaming in a hostile environment (e.g., a battlefield) with relatively poor physical protection, have non-negligible probability of being compromised. Therefore, we should not only consider malicious attacks from outside a network, but also take into account the attacks launched from within the network by compromised nodes. Therefore, to achieve high survivability, ad hoc networks should have a distributed architecture with no central entities. Introducing any

ISSN (Online) : 2229-6166

Volume 4 Issue 3 September 2013

central entity into our security solution could lead to significant vulnerability; that is, if this centralized entity is compromised, then the entire network is subverted.
Thirdly, an ad hoc network is dynamic because of frequent changes in both its topology and its membership (i.e., nodes frequently join and leave the network). Trust relationship among nodes also changes, for example, when certain nodes are detected as being compromised. Unlike other wireless mobile networks, such as mobile IP [1,2,3], nodes in an ad hoc network may dynamically become affiliated with administrative domains. Any security solution with a static configuration would not suffice. It is desirable for our security mechanisms to adapt on-the-fly to these changes. Finally, an ad hoc network may consist of hundreds or even thousands of nodes. Security mechanisms should be scalable to handle such a large network

3. PROTOCOLS FOR MANET

3.1 Classification of MANET Routing Protocols

3.1.1 Flat Routing

Flat routing protocols are divided mainly into two classes; the first one is Proactive (Table-Driven) routing protocols and other is Reactive (On-Demand) routing protocols. One thing general for both protocol classes is that every node participating in routing plays an equal role. Proactive routing is mostly based on LS (Link-State) while On-Demand routing is based on DV (Distance-Vector).

3.1.2Geographical Routing Protocols

Geographic routing protocols prevent network-wide searches for destinations. If the recent geographical coordinates are known then control and data packets can be sent in the general direction of the destination. This trim downs control overhead in the network.

There are two approaches to geographic mobile ad-hoc networks: (1) Actual geographic coordinates (as obtained through GPS – the Global Positioning System) (2) Reference points in some fixed coordinate system. Some of these routing protocols are:

- Distance Routing Effect Algorithm for Mobility (DREAM)
- GPS Ant-Like (GPSAL)
- Greedy Perimeter Stateless Routing (GPSR)

ISSN (Online) : 2229-6166

Volume 4 Issue 3 September 2013

There is another category of routing protocols; known as Power Aware routing protocols . This type of routing protocols take into consideration the energy required to transmit a signal, because the energy required is proportional to the square of the distance and transmitting a signal half the distance requires one fourth of the energy. Power Aware Multi Access Protocol with Signaling Ad-hoc Network (PAMAS) is an example of these types of routing protocol.

3.2 Description of Reactive Protocols

Reactive protocol is identified as On-Demand protocols because it creates routes only when these routes are needed. The various Reactive routing protocols are discussed below:

3.2.1 Ad-hoc On-Demand Distance Vector (AODV)

Ad-hoc On-Demand Distance Vector (AODV) is a routing protocol for mobile ad-hoc networks. The AODV routing protocol is a Reactive routing protocol; therefore, routes are determined only when needed. The AODV algorithm gives an easy way to get change in the link situation. For example if a link fails notifications are sent only to the affected nodes in the network. This notification cancels all the routes through this affected node. It builds unicast routes from source to destination and that's why the network usage is least. In AODV traffic is minimum as routes are establishes On-Demand. AODV does not allow keeping extra routing which is not in use .

3.2.2 Dynamic Source Routing (DSR)

Dynamic Source Routing (**DSR**) is a routingprotocol for wireless mesh networks. It is similar to AODV in that it forms a route on-demand when a transmitting computer requests one. However, it uses source routing instead of relying on the routing table at each intermediate device.

Determining source routes requires accumulating the address of each device between the source and destination during route discovery. The accumulated path information is cached by nodes processing the route discovery packets. The learned paths are used to route packets. To accomplish source routing, the routed packets contain the address of each device the packet will traverse. This may result in high overhead for long paths or large addresses, like IPv6. To avoid using source routing, DSR optionally defines a flow id option that allows packets to be forwarded on a hop-by-hop basis.

This protocol is truly based on source routing whereby all the routing information is maintained (continually updated) at mobile nodes. It has only two major phases, which are Route Discovery and Route Maintenance. Route Reply would only be generated if the message has reached the intended destination node (route record which is initially contained in Route Request would be inserted into the Route Reply).

ISSN (Online) : 2229-6166

Volume 4 Issue 3 September 2013

To return the Route Reply, the destination node must have a route to the source node. If the route is in the Destination Node's route cache, the route would be used. Otherwise, the node will reverse the route based on the route record in the Route Request message header (this requires that all links are symmetric). In the event of fatal transmission, the Route Maintenance Phase is initiated whereby the Route Error packets are generated at a node. The erroneous hop will be removed from the node's route cache; all routes containing the hop are truncated at that point. Again, the Route Discovery Phase is initiated to determine the most viable route.

3.2.3 Temporally-ordered routing algorithm(TORA)

The TORA[3] attempts to achieve a high degree of scalability using a "flat", non-hierarchical routing algorithm. In its operation the algorithm attempts to suppress, to the greatest extent possible, the generation of far-reaching control message propagation. In order to achieve this, the TORA does not use a shortest path solution, an approach which is unusual for routing algorithms of this type.

TORA builds and maintains a Directed Acyclic GraphDAG rooted at a destination. No two nodes may have the same height.

Information may flow from nodes with higher heights to nodes with lower heights. Information can therefore be thought of as a fluid that may only flow downhill. By maintaining a set of totally-ordered heights at all times, TORA achieves loop-free multipath routing, as information cannot 'flow uphill' and so cross back on itself.

The key design concepts of TORA is localization of control messages to a very small set of nodes near the occurrence of a topological change. To accomplish this, nodes need to maintain the routing information about adjacent (one hop) nodes. The protocol performs three basic functions:

- Route creation
- Route maintenance
- Route erasure

During the route creation and maintenance phases, nodes use a height metric to establish a directed acyclic graph (DAG) rooted at destination. Thereafter links are assigned based on the relative height metric of neighboring nodes. During the times of mobility the DAG is broken and the route maintenance unit comes into picture to reestablish a DAG routed at the destination.

Timing is an important factor for TORA because the height metric is dependent on the logical time of the link failure.

TORA's route erasure phase is essentially involving flooding a broadcast clear packet (CLR) throughout the network to erase invalid routes

4. ATTACKS ON MANET ROUTING PROTOCOLS

The nature of attacks [4,5] vary greatly from one set of circumstances to another. In general, there is flow of information from a source to a destination. We have listed below the generic types of attack that might be encountered. They have also been pictorially depicted.

Interruption: An asset of the system is destroyed, becomes unavailable or unusable. This is an attack on availability. Examples include destruction of a piece of hardware, or cutting of a communication line.

Interception: An unauthorized party gains access to an asset. This is an attack[6] on confidentiality. The unauthorized party could be a person, a program or a computer. Examplesinclude wiretapping to capture data in a network and the illicit copying of files or programs.

Modification: An unauthorized party not only gains access to but tampers with an asset.This is an attack on integrity. Examples include changing values in a data file or modifying the contents of a message being transmitted in a network.

Fabrication: An unauthorized party inserts counterfeit objects into the system. This is anattack on authentication. Examples include the insertion of spurious messages in a network or the addition of records to a file.

Interruption: An asset of the system is destroyed, becomes unavailable or unusable. This is an attack on availability. Examples include destruction of a piece of hardware, or cutting of a communication line.

Interception: An unauthorized party gains access to an asset. This is an attack on confidentiality[7]. The unauthorized party could be a person, a program or a computer. Examplesinclude wiretapping to capture data in a network and the illicit copying of files or programs.

Modification: An unauthorized party not only gains access to but tampers with an asset.This is an attack on integrity. Examples include changing values in a data file or modifying the contents of a message being transmitted in a network.

Fabrication: An unauthorized party inserts counterfeit objects into the system. This is anattack on authentication. Examples include the insertion of spurious messages in a network or the addition of records to a file.

ISSN (Online) : 2229-6166

Volume 4 Issue 3 September 2013

5. CONCLUSION

Currently, ad hoc routing protocols are vulnerable to several kinds of attacks. Also, existing security enhancement techniques such as the Non-Disclosure Method and IPsec can be considered but these are either too expensive or ineffective to be of value. Unless protection against routing attacks can be provided by the applications that are used in the network, current routing protocols should not be used in areas of applications where the threats of denial-of-service attacks, forged routes, or location disclosure are of any significant importance. Ad hoc networking is still a raw area of research as can be seen with the problems that exist in these networks and the emerging solutions. Several protocols for secured routing in Ad-hoc networks have been proposed. There is a need to make them more secure and robust to adapt to the demanding requirements of these networks. The current security mechanisms, each defeats one or few routing attacks. It is still a challenging task to design routing protocols resistant to multiple attacks.

6. REFERENCES

[1] J. Ioannidis, D. Duchamp, and J. M. Gerald Q. IP based protocols for mobile networking. ACM SIGCOMM Computer Communication Review (SIGCOMM'91), 21(4):235–245, September 1991.

[2] F. Teraoka, Y. Yokore, and M. Tokoro. A network architecture providing host migration transparency. ACM SIGCOMM Computer Communication Review (SIGCOMM'91), 21(4):209–220, September 1991.

[3] C. E. Perkins. IP mobility support. Request for Comments: 2002, October 1996.

[4] A.Kush, C.Hwang, P.Gupta, "Secured Routing Scheme for Adhoc Networks" International Journal of Computer Theory and Engineering (IJCTE). May 2009, Volume 3.pp 1793-179

[5] A.Kush, C.Hwang, "Proposed Protocol For Hash-Secured Routing in Ad hoc Networks", MASAUM JOURNAL OF COMPUTING (MJC) Volume: 1 Issue: 2 Month: September 2009 , pp 221-226.

[6]Krishna Ramachandran. Aodv-st.Technical report, University of California, Santaarbara, USA. http://www.cs.ucsb.edu/ krishna/aodv-st/(visited 2006-04-15).

[7]BassamHalabi. Internet Routing Architectures.Cisco Press, 2000.