RESEARCH ARTICLE OPEN ACCESS

A Survey Secure Routing Protocols Mobile AdHoc Network

Shameer Mohamad[1], Imran Khan[2]

1(Computer Science and Engineering,Dhanalakshmi College of Engineering,Chennai)

Abstract:

Mobile Ad hoc Networks are assortment of mobile terminals or nodes, allowing no stationary infrastructure and centralized administration. Several routing protocols have been proposed in recent years for possible deployment of Mobile Ad hoc Networks (MANETs) in military, government and commercial applications. The strength of its infrastructure (wireless nature) also becomes the point of its greatest vulnerability. Thus decreasing the confidence level of the system as it pertains to availability, reliability, data integrity and privacy concerns. Protocols are introduced for improving the routing mechanism to find route between any source and destination host across the network. In this paper we present a survey on routing protocols and we review OLSR protocol and improvements on this protocol.

Keywords — **Ad hoc networks, routing protocols, security, wireless systems, mobile routing..**

I. Introduction:

In the next generation of wireless communication systems, there is a tremendous need for the rapid deployment of independent mobile users. Mobile Ad hoc Network (MANET) is a set of mobile devices (nodes), which over a shared wireless medium communicate with each other without the presence of a predefined infrastructure or a central authority. Due to no stationary infrastructure, all nodes can move freely, topology may change rapidly and unpredictably over time, and nodes have to form their own mutual infrastructures. The security of communication in ad hoc wireless networks is important, especially in military applications. The absence of any central coordination mechanism and shared wireless medium makes MANETs more vulnerable to digital/cyber attacks than wired networks. Designing of routing protocol in AdHoc network depends various factors like mobility, bandwidth, resource constraint, hidden and exposed terminal problems etc. Thus, routing protocol is structured for purposes such as fully distributed, adaptive frequent and stable topology, loop free and minimum number of collisions.

DSR Protocol:

The Dynamic Source Routing protocol (DSR) is a simple and efficient routing protocol designed specifically for use in multi-hop wireless ad hoc networks of mobile nodes. DSR allows the network to be completely self-organizing and self-configuring, without the need for any existing network infrastructure or administration. The protocol is composed of the two mechanisms of Route Discovery and Route Maintenance, which work together to allow nodes to discover and maintain source routes to arbitrary destinations in the ad hoc network. Dynamic source routing protocol (DSR) is an on-demand protocol designed to restrict the bandwidth consumed by control packets in ad hoc wireless networks by eliminating the periodic table-update messages required in the table-driven approach. The major difference

between this and the other on-demand routing protocols is that it is beacon-less and hence does not require periodic hello packet (beacon) transmissions, which are used by a node to inform its neighbors of its presence. The basic approach of this protocol (and all other on-demand routing protocols) during the route construction phase is to establish a route by flooding Route Request packets in the network. The destination node, on receiving a Route Request packet, responds by sending a Route Reply packet back to the source, which carries the route traversed by the Route Request packet received.

AODV Protocol:

An adhoc network is the cooperative engagement of a collection of mobile nodes without the required inter vention of any centralized access point or existing in frastructure In this paper we present Adhoc On Demand Distance Vector Routing AODV a novel algorithm for the operation of such adhoc networks Each Mobile Host operates as a specialized router and routes are obtained as needed ondemand with little or no reliance on periodic advertisements Our new routing algorithm is quite suitable for a dynamic self starting networkas required by users wishing to utilize adhoc networks. The AODV (Ad-Hoc On-Demand Distance Vector) routing protocol is a reactive routing protocol that uses some characteristics of proactive routing protocols. Routes are established on-demand, as they are needed. However, once established a route is maintained as long as it is needed. Reactive (or on-demand) routing protocols find a path between the source and the destination only when the path is needed (i.e., if there are data to be exchanged between the source and the destination). An advantage of this approach is that the routing overhead is greatly reduced. A disadvantage is a possible large delay from the moment the route is needed (a packet is ready to be sent) until the time the route is actually acquired.

DSDV Protocol:

DSDV (Destination-Sequenced Distance Vector Routing DSDV) is a table driven routing scheme. Its based on Bellman-Ford algorithm. Each entry in the routing table contains a sequence number which is generated by the destination by the destination and the emitter needs to send out the next update using this number. Routing information is distributed between nodes by sending full dumps infrequently and smaller incremental updates more frequently.

II. Routing Algorithms Comparisons:

DPRAODV Protocol:

DPRAODV received signal is higher than the threshold value, then the sender node is regarded as black hole node and then a blacklist is constructed with the attacker node increases the packet delivery ratio with nominal increase in routing overhead. This method cannot detect the cooperative black hole attacks. Also the false detection ratio of this scheme is high.

- **Secure Adhoc Routing:**

Ad hoc network routing protocols have been based in part on distance vector approaches, they have generally assumed a trusted environment. In this research project, we design and evaluate the Secure Efficient Ad hoc Distance vector routing protocol (SEAD), a secure ad hoc network routing protocol based on the design of the Destination-Sequenced Distance-Vector routing protocol (DSDV).

- **Intrusion Detection System:**

An intrusion detection system (IDS) is a device or software application that monitors network or system activities for malicious activities or policy violations and produces

reports to a management station. IDS come in a variety of "flavors" and approach the goal of detecting suspicious traffic in different ways. There are network based (NIDS) and host based (HIDS) intrusion detection systems. Some systems may attempt to stop an intrusion attempt but this is neither required nor expected of a monitoring system. Intrusion detection and prevention systems (IDPS) are primarily focused on identifying possible incidents, logging information about them, and reporting attempts

Gray Hole Attack

This usually occurs from a router becoming compromised from a number of different causes. One cause mentioned in research is through a denial-of-service attack on the router using a known DDOS tool. Because packets are routinely dropped from a lossy network, the packet drop attack is very hard to detect and prevent.

Attacks on AODV Protocol:

At the start of communication routes are generated by Network Each and every node has its own sequence number, and this number increases whenever a link changes. Sends a route request (RREQ) message by using broadcasting. The RREQ ID increases by one every time node S sends an RREQ message If they have a valid route to the destination, then they send an RREP message to node.

Bootstrapping Security Associations for Routing:

A Cyclic Dependency Problem: Routing service depends on security services to authenticate the source of a message (i.e., its IP address) and the message content. To acquire secure bindings between a node‟s IP address and key, it must either reach a trustedauthority node or establish trust relationships with other nodes without relying on trusted authorities.

Breaking the Cyclic Dependency : We remove dependency by using a secure binding mechanism for establishing secure node-tonode associations that is independent of secure routing and other security services. Idea of a secure binding between an IP address and a key that is independent of any other security services by control messages of MIPv6.

Intrusion Detection:

The Optimized Link State Routing (OLSR) protocol is a proactive Mobile Ad hoc Network (MANET) routing protocol.

The OLSR Protocol:

The protocol is an optimization of the classical link state algorithm tailored to the requirements of a mobile wireless LAN. The key concept used in the protocol is that of multipoint relays (MPRs). MPRs are selected nodes which forward broadcast messages during the flooding process. This technique substantially reduces the message overhead as compared to a classical flooding mechanism, where every node retransmits each message when it receives the first copy of the message. In OLSR, link state information is generated only by nodes elected as MPRs. Thus, a second optimization is achieved by minimizing the number of control messages flooded in the network. As a third optimization, an MPR node may chose to report only links between itself and its MPR selectors.

PRISM: Privacy-friendly Routing in Suspicious MANETs (and VANETs):

Mobile Ad-Hoc Networks (MANETs) play an increasingly important role in many environments and applications, especially, in critical settings that lack fixed network infrastructure, such as: emergency rescue,

humanitarian aid, as well as military and law enforcement.

Privacy aspects of mobility. Unlike most networks, where communication is based on long-term identities (addresses), we argue that the location-centric communication paradigm is better-suited for privacy in suspicious MANETs. To this end, we construct an on-demand location-based anonymous MANET routing protocol (PRISM) that achieves privacy and security against both outsider and insider adversaries. We analyze security, privacy and performance of PRISM and compare it to alternative techniques. Results show that PRISM is more computationally efficient and offers better privacy than prior work.

Application Examples: Military and law-enforcement MANETs are compelling examples of settings where privacy, in addition to security, is very important. Zooming in on the military example, one can imagine a battlefield MANET composed of different types of nodes, like infantry soldiers, vehicles, and aircrafts as well as other types of personnel and equipment.

Reference:

[1] A. Fatemeh Sarkohaki, B. Shahram Jamali " A Survey of Routing Protocols for Mobile AdHoc Networks with Comprehensive Study of OLSR" International journal of Computer Science & Network Solutions- 2014.

[2] S. Sutha , Dr. B. Anandhi "Routing Protocols towards Security objective of Mobile Adhoc Networks – A Survey" IJISET - International Journal of Innovative Science, Engineering & Technology, Vol. 1 Issue 8, October 2014

[3] Sudhir Agrawal, Sanjeev Jain, Sanjeev Sharma "A Survey of Routing Attacks and Security Measures in Mobile Ad-Hoc Networks" Journal of computing, volume 3, issue 1, January 2011, 2151-9617.

[4] Loay Abusalah, Ashfaq Khokhar, and Mohsen Guizani "A Survey of Secure Mobile Ad Hoc Routing Protocols" IEEE communications surveys & tutorials, vol. 10, no. 4, fourth quarter 2008.

[5] S.Ranjithkumar, N. Thillaiarasu, "A Survey of Secure Routing Protocols of Mobile AdHoc Network" International Journal of Computer Science and Engineering – volume 2 issue 2 February 2015.

[6] V. Shanmuganathan Mr.T.Anand "A Survey on Gray Hole Attack in MANET " IRACST – International Journal of Computer Networks and Wireless Communications (IJCNWC), ISSN: 2250-3501.