Volume 4, Issue 4, April 2014 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Survey of Challenges and Solutions in MANET

Karamjeet Singh*, Nancy Garg
Department of Computer Science
University College Kurukshetra University Kurukshetra, India

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, Attacks, MANETs.

I INTRODUCTION

A Mobile Ad Hoc Network (MANET) is a network consisting of a collection of nodes capable of communicating with each other without help from a network infrastructure. The network is decentralized, where all network activity, including discovering the topology and delivering messages must be executed by the nodes themselves. Hence routing functionality will have to be incorporated into the mobile nodes. Since the nodes communicate over wireless links, they have to contend with the effects of radio communication, such as noise, fading, and interference. The vision of mobile ad hoc networking is to support robust and efficient operation in mobile wireless networks by incorporating routing functionality into mobile nodes. Such networks are envisioned to have dynamic, sometimes rapidly-changing, random, multihop topologies which are likely composed of relatively bandwidth-constrained wireless links. Applications of MANETs include the battlefield applications, rescue work, as well as civilian applications like an outdoor meeting, or an ad-hoc classroom. With the increasing number of applications to harness the advantages of Ad Hoc Networks, more concerns arise for security issues in MANETs.

II VULNERABILITIES IN MANET

The mobile ad hoc networks have far more vulnerabilities than the traditional wired networks, security is much more difficult to maintain in the mobile ad hoc network than in the wired network.

- **Lack of Secure Boundaries**

There is not such a clear secure boundary in the mobile ad hoc network, which can be compared with the clear line of defense in the traditional wired network. In the mobile ad hoc network, there is no need for an adversary to gain the physical access to visit the network: once the adversary is in the radio range of any other nodes in the mobile ad hoc network, it can communicate with those nodes in its radio range and thus join the network automatically. As a result, the mobile ad hoc network does not provide the so-called secure boundary to protect the network from some potentially dangerous network accesses. The mobile ad hoc network suffers from all-weather attacks, which can come from any node that is in the radio range of any node in the network, at any time, and target to any other node(s) in the network.

- **Threats from Compromised nodes In the Network**

Routing algorithms for MANETs usually assume that nodes are cooperative and non malicious. As a result, a malicious attacker can easily become an important routing agent and disrupt network operations by disobeying the protocol specifications. For example, a node can pose as a neighbor to other nodes and participate in collective decision-making mechanisms, possibly affecting networking significantly.

- **Unavailability of Centralized Management Facility**

The absence of centralized management machinery makes the detection of attacks a very difficult problem because it is not easy to monitor the traffic in a highly dynamic and large scale ad hoc network. The lack of centralized management machinery will impede the trust management for the nodes in the ad hoc network [4]. In mobile ad hoc network, all the nodes are required to cooperate in the network operation, while no security association (SA2) can be assumed for all the network nodes. , some algorithms in the mobile ad hoc network rely on the cooperative participation of all nodes and the infrastructure. Because there is no centralized authority, and decision making in mobile ad hoc network is sometimes decentralized, the adversary can make use of this vulnerability and perform some attacks that can break the cooperative algorithm [5].In one word, the absence of centralized management machinery will cause vulnerability that can influence several aspects of operations in the mobile ad hoc network.

Restricted Resources

Resource constraints are a further vulnerability. The nodes in the mobile ad hoc network need to consider the restricted battery power, which will cause several problems. There can be a variety of devices on MANETs, ranging from laptops to handheld devices such as PDAs and mobile phones. These will generally have different computing and storage capacities that can be the focus of new attacks. Battery power with different capacities is used by the mobile nodes. For example, mobile nodes generally run on battery power. This has led to emergence of innovative attacks targeting this aspect. This is a challenge for networks that are already resource-constrained.

Scalability

The traditional wired network in that its scale is generally predefined when it is designed and will not change much during the use, the scale of the ad hoc network keeps changing all the time: because nodes can leave and join the network, and move independently. So you can hardly predict how many nodes there will be in the network in the future. As a result, the protocols and services that are applied to the ad hoc network such as routing protocol and key management service should be compatible to the continuously changing scale of the ad hoc network, which may range from decades of nodes to hundreds of nodes, or even thousands of nodes. In other words, these protocols and services need to scale up and down efficiently.

III **Existing Protocols in MANET**

Routing protocols are used to provide communication within the network. These Protocols find a route for packet delivery and deliver the packet to the correct destination. The primary goal of such an ad-hoc network routing protocol is correct and efficient route establishment between a pair of nodes so that messages may be delivered in a timely manner. Routing protocols for MANETs can be broadly classified into three main categories:-

1.) Proactive(Table Driven) routing protocols:- Every node in the network has one or more routes to any possible destination in its routing table at any given time. Certain Proactive Routing Protocols are DSDV, Wireless Routing Protocol (WRP), Global State Routing (GSR) and Cluster-head Gateway Switch Routing (CGSR).

2.) Reactive(On Demand) routing protocols:- 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. Some Reactive Protocols are Cluster Based Routing Protocol (CBRP), AODV, DSR, TORA, Associativity-Based Routing (ABR), Signal Stability Routing (SSR) and Location Aided Routing (LAR).

Description of Proactive or Table Driven Protocols:

- **Dynamic Destination-Sequenced Distance-Vector Routing Protocol (DSDV)**

The Destination-Sequenced Distance-Vector (DSDV) Routing Algorithm is based on the idea of the classical Bellman-Ford Routing Algorithm with certain improvements. DSDV finds shortest paths between nodes using a distributed version of the Bellman-Ford algorithm. Each node maintains a routing table, with an entry for each possible destination in the network, the number of hops required to reach the destination and the sequence number of the information received regarding that destination, and stamped by the destination. The sequence number is used to distinguish stale routes from new ones and thus avoid the formation of loops. The stations periodically transmit their routing tables to their immediate neighbors. A station also transmits its routing table if a significant change has occurred in its table from the last update sent. So, the update is both time-driven and event-driven. [6,7].

- **The Wireless Routing Protocol (WRP)**

The Wireless Routing Protocol (WRP) s a table-based loop-free distance-vector routing protocol. Each node in the network maintains a Distance table, a Routing table, a Link-Cost table and a Message Retransmission list(MRL). Each entry of the MRL contains the sequence number of the update message, a retransmission counter, an acknowledgment required flag vector with one entry per neighbor, and a list of updates sent in the update message. The MRL records which updates in an update message need to be retransmitted and which neighbors should acknowledge the retransmission General route updates are sent among neighboring nodes with distance and second-to-last hop information for each destination, resulting in faster convergence. [8] This the protocol introduces mechanisms which reduce route loops and ensure reliable message exchange. WRP, like DSDV, maintains an up-to-date view of the network, every node has a readily available route to every destination node in the network. It differs from DSDV in table maintenance and in the update procedures.

- **Global State Routing**

Global State Routing (GSR) [9] is a uniform, topology oriented, proactive routing protocol. Global State Routing (GSR) is similar to DSDV. It is a variant of traditional link-state protocols, in which each node sends link-state information to every node in the network each time its connectivity changes. In this algorithm, each node maintains a Neighbor list, a Topology table, a Next Hop table and a Distance table. Neighbor list of a node contains the list of its neighbors (here all nodes that can be heard by a node are assumed to be its neighbors.). For each destination node, the Topology table contains the link state information as reported by the destination and the timestamp of the information. For each destination, the Next Hop table contains the next hop to which the packets for this destination must be forwarded. The Distance table contains the shortest distance to each destination node. The routing messages are generated on a link change as in link state protocols. On receiving a routing message, the node updates its Topology table if the sequence number of the message is newer than the sequence number stored in the table. After this the node

reconstructs its routing table and broadcasts the information to its neighbors. GSR uses some further developed techniques to broadcast the control messages, unlike other Link State protocols GSR only broadcast control messages to its neighbor rather than broadcasting to the whole network, which reduces the amount of control messages transmitted throughout the network. As a results the message size became relatively larger than other messages format used in other Link State protocols and as the network size get bigger these message get bigger size which uses high amount of bandwidth to transmit the update messages.

- **CGSR**

Cluster head Gateway Switch Routing protocol [10] is a multichannel operation capable protocol. It enables code separation among clusters. The clusters are formed by cluster head election procedure, which is quite intensive process. On that reason the protocol uses so called Least Cluster Change (LCC) algorithm for that election. By using LCC can cluster heads only changed when two cluster heads come into contact with each other or when a node moves out of contact of all other cluster heads. CGSR is not an autonomous protocol. It uses DSDV as the underlying routing scheme. The DSDV approach is modified to use a hierarchical cluster head-to-gateway routing. A packet sent by a node is first routed to its cluster head, and then the packet is routed from the cluster head to a gateway to another cluster head, until the destination node's cluster head is reached. That destination cluster head then transmits the packet to the destination node.

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:

- **AODV**

The Ad-hoc On-demand Distance Vector (AODV) routing protocol is a routing protocol used for dynamic wireless networks where nodes can enter and leave the network at will. To find a route to a particular destination node, the source node broadcasts a RREQ to its immediate neighbors. If one of these neighbors has a route to the destination, then it replies back with a RREP. Otherwise the neighbors in turn rebroadcast the request. This continues until the RREQ hits the final destination or a node with a route to the destination. At that point a chain of RREP messages is sent back and the original source node finally has a route to the destination. AODV is an 'on demand routing protocol' with small delay. That means that routes are only established when needed to reduce traffic overhead. AODV supports Unicast, Broadcast and Multicast without any further protocols. The Count-To-Infinity and loop problem is solved with sequence numbers and the registration of the costs. In AODV every hop has the constant cost of one. The routes age very quickly in order to accommodate the movement of the mobile nodes. Link breakages can locally be repaired very efficiently.

- **DSR**

The Dynamic Source Routing (DSR) [8] protocol is a distance-vector routing protocol for MANETs. When a node generates a packet to a certain destination and it does not have a known route to that destination, this node starts a route discovery procedure. Therefore, DSR is a reactive protocol. One benefit of DSR is that no periodic routing packets are required. DSR also has the capability to handle unidirectional links [11]. Since DSR dis- covers routes on-demand, it may have poor performance in terms of control overhead in networks with high mobility and heavy traffic loads. Scalability is said to be another disadvantage of DSR, because DSR relies on blind broadcasts to discover routes.

To handle unreliable transmissions of control messages, DSR either relies on the underlying MAC protocol to provide guaranteed delivery or it retransmits control messages for a certain number of times. Since DSR is a reactive protocol, it cannot tell whether a destination is unreachable or the route request is lost. Therefore, it suffers more over- head if the underlying MAC layer does not support guaranteed delivery [12]. This is a common problem for reactive routing protocols because when no reply message is heard, routers with a reactive routing protocol cannot tell the difference between the case of a transmission error and the case of unreachable nodes. Reactive routing protocols try to use extra acknowledgements or a small number of retransmissions to solve this problem and, thus, introduce more overhead. Proactive routing protocols periodically broadcast control messages and remove local routing entries if they time out. Hence, they do not have this problem. But, of course, the periodically broadcast control messages con- tribute to overhead [13].

- **Temporarily Ordered Routing Algorithm (TORA)**

TORA [14] is a reactive routing protocol with some proactive enhancements where a link between nodes is established creating a Directed Acyclic Graph (DAG) of the route from the source node to the destination. This protocol uses a ,,,,link reversal"""" model in route discovery. A route discovery query is broadcasted and propagated throughout the network until it reaches the destination or a node that has information about how to reach the destination. TORA uses an arbitrary height metric to establish a direct acyclic graph (DAG) and the length of the route that physically (DAG) rooted at the destination. In TORA three steps are involved in establishing a network.

• Creating the routes from source to destination,
• Maintaining the routes
• Erasing invalid routes.

[15]TORA has a unique feature of maintaining multiple routes to the destination so that topological changes do not require any reaction at all. The protocol reacts only when all routes to the destination are lost. In the event of network partitions the protocol is able to detect the partition and erase all invalid routes. To initiate a route, the node broadcasts a QUERY packet to its neighbors. This QUERY is rebroadcast through the network until it reaches the destination or an

inter-mediate node that has route to the destination. The recipient of the QUERY packet then broadcast the UPDATE packet which lists its height with respect to the destination.

IV 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.

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 an attack on authentication. Examples include the insertion of spurious messages in a network or the addition of records to a file.

V. 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.

ACKNOWLEDGMENT

W express my sincere and deep sense of gratitude to Dr. Sima and other contributors for there guidance and constant encouragement which have been used in the preparation of this paper. It is my great pleasure to acknowledge gratefully the debt of all of my computer science department colleagues who helped in completion of this paper.

REFERENCES:

[1] Park VD, Corson MS (1997) A highly adaptive distributed routing algorithm for mobile wireless networks. Proceedings of IEEE INFOCOM 1997, Volume 3:1405–1413 Haas ZJ

[2] P.Visalakshi, 1 S.Anjugam2 "Security issues and vulnerabilities in Mobile Ad hoc Networks (MANET)-A Survey" International Journal of Computational Engineering Research (IJCER) ISSN: 2250-3005

[3] Wenjia Li and Anupam Joshi "Security Issues in Mobile Ad Hoc Networks" www.csee.umbc.edu/~wenjia1

[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] Padmini Misra, Routing Protocols for Ad Hoc Mobile Wireless Networks, misra @ cse . wustl.eduhttp://www.cse.wustl.edu/~jain/cis788-99/ftp/adhoc_routing/

[7] Vijendra Rai," Simulation of Ad-hoc Networks Using DSDV, AODV And DSR Protocols And Their Performance Comparison" Proceedings of the 4th National Conference; INDIACom-2010Computing For Nation Development, February 25 – 26, 2010

[8] Vishal Gupta, "Comparative Performance Analysis of AODV, DSR, DSDV, LAR1 and WRP Routing Protocols in MANET using GloMoSim 2.0.3 Simulator" International Journal of Computer Applications (0975 – 8887) Volume 52– No.20, August 2012

[9] T. Chen, M. Gerla, "Global State Routing: A new Routing Scheme for Ad-Hoc Wireless Networks", Proceedings of IEEE ICC'98, pages 171-175, August 1998. http: // www 1.ics. uci. edu/~atm/adhoc/papercollection/papers.html

[10] C.C. Chiang, H.K. Wu, W. Liu, M. Gerla, "Routing in Clustered Multihop Mobile Wireless Networks with Fading Channel", Proceeding of IEEE Singapore International Conference on Networks SICON'97, pages 197-212, April 1997. http://www1.ics.uci.edu/~atm/adhoc/papercollection/gerla-routing-clustered-sicon97.pdf

[11] Nayyar Anand; "Simulation Based Evaluation of Reactive Routing Protocols of MANET", IEEE Second International Conference on Advanced Computing & Communication Technologies 2012, pp. 561-568, 2012.

[12] Khatkar Avni, Singh Yudhvir; "Performance Evaluation of Hybrid Routing Protocols in Mobile Adhoc Networks", IEEE Second International Conference onAdvanced Computing & Communication Technologies 2012, pp. 542-545, 2012.

[13] Vetrivelan N. and Reddy A.V., 2008. "Performance Analysis of Three routing Protocols for Varying MANET Size", Proceedings of the International Multi-Conference of Engineers and Computer Scientists.

