Ghasem Farjamnia, Mehdi Zekriyapanah Gashti / International Journal of Engineering Research and Applications (IJERA) ISSN: 2248-9622 www.ijera.com
Vol. 3, Issue 1, January -February 2013, pp.1916-1919

Investigation of routing protocols and group members reliability in MANET

Ghasem Farjamnia*, Mehdi Zekriyapanah Gashti**
Department of Computer Engineering, Payame Noor University, I.R of IRAN

ABSTRACT

Investigation of routing protocols and group members' reliability in Ad hoc or MANET by making a multi-step wireless network with a specific structure and out of sight connection provides a good framework for achievement of subjective objectives. In architecture of such network there is no fixed and specified structure available and the nodes are mobile. Some of the existing challenges in these networks are included of: discussion on finding node's position, routing and way of their safe sending, etc that in this paper we will proceed.

Keywords - **MANET, Topology-based routing, Position-based routing protocols, Security, Categorizing Ad Hoc.**

I. INTRODUCTION

Historically Mobile Ad hoc Networks (MANET) were applied in order to improve communications in war field. Dynamic nature of military operations made it impossible to rely on achievement of a fix communicative structure in the war field. Wireless relations have also limitations due to possibility of interferences in radio signals and the radio frequencies higher than 100MHZ are hardly diffused over the LOS (Line of Sight) [1]. By making a multi-step mobile network without specified structure and LOS connection would provide an appropriate framework to achieve subjective objectives. There are a lot of problems in the field of design and development of network algorithms for supporting networks with ten thousands of nodes, which can resist against security threats and it uses small, inexpensive and low radio messages to support complex packet transmission protocols [1]. Some efforts in this regard led to design of Low-cost Packet Radio (LPR) in 1987 [2]. In this technology, a group of advanced network management protocols were developed and a topology of hierarchical network based on dynamic clustering was applied to support network development capacity. At the end of 1980 and beginning of 1990s, growth of Internet structure and microcomputer revolution created a Packet Radio network [1].

In 1994, a program called DARPA Global Mobile (GloMo) Information Systems [3] started along penetration of general information structure in a mobile wireless environment by DOD which was designed for supporting multimedia connection from Ethernet type at any time and place between wireless equipments.

Extending the Littoral Battle-space Advanced Concept Technology Demonstration (ELBACTD) is another MANET development discovery in 1999 for investigating the possibility of operations for Navy Forces needing connection on horizontal line of ships overboard to headquarters at beach via an aerial sustainment. Approximately 20 nodes are organized to be applied for Lucent's Wave LAN and VRC-99A that are applied for construction of access connections and Backbone network. ELB ACTD has been successful in proving the use of aerial sustainment's for connection of users without existence of LOS. In the middle of 1990, standards of commercial Radio technologies such as IEEE 802.11 [4] entered the market and the objectives of MANET exceeded the military and war issues. Many existing MANET systems developed beyond military issues in developed academic environments, however recently business based solutions such as Mesh Networks and SPAN works have emerged too.

II. CATEGORIZING AD HOC NETWORKS

In recent years, vast access to wireless connections have simulated some searches on self-organized networks which do not require a predetermined infrastructure, these networks are called Ad Hoc networks. They are generally a set of independent nodes which cooperate with each other in transmission of data. These nodes usually act as final systems and routers in a simultaneous time.

Ad Hoc networks are categorized in two statistic and mobile classes. In statistic Ad Hoc networks, when a

node becomes a member of network, the position of the node cannot be changed any more. A sample of statistic Ad Hoc networks is Rooftop [5]; like Nokia Rooftop and (samples of Rooftop ad hoc wireless networks). In mobile Ad Hoc networks, systems may move voluntarily. Mobile Ad Hoc networks are used for making connections between vehicles. In the continue we will explain routing methods in mobile Ad Hoc networks.

III. ROUTING IN MOBILE AD HOC NETWORKS

Since the topology of mobile Ad Hoc networks changes permanently and without previous notice, routing in such networks is a challenge, two topology-based routing and position-based methods exist in such networks that we will explain as follow:

III.I. TOPOLOGY-BASED ROUTING

Topology-based routing protocols use data on existing links in network for Packet Forwarding. These protocols are categorized to three groups of Proactive or Table-Driven and Reactive or On-Demand and Hybrid methods.

III.I.I. PROACTIVE ROUTING METHODS

In Proactive routing methods each node keeps the routing data to the other nodes of network. Routing data are usually kept in some different tables; these tables are updated frequently or by the change in network's topology. The difference between the protocols of this class is in method updating routing data and type of data kept in each routing table, besides that, each routing protocol can keep a different number of tables.

The main weakness of such methods is that they keep routs which are immediate or are not currently used and this occupies a vast part of bandwidth when network's topology changes permanently. [6] OLSR [7] TBRPF are samples of routing protocols.

III.I.II. REACTIVE ROUTING PROTOCOLS

In reactive routing protocols, each node keeps the routing data which is currently used and this reduces network's overhead. Protocols such as DSR [8], TORA [9] and AODV [10] are samples of reactive routing protocols.

III.I.III. HYBRID ROUTING PROTOCOLS

A combination of proactive routing protocols and reactive routing protocols reach to a higher level of efficiency and extensibility, this combination has created Hybrid routing protocols. However, even a combination of two strategies still requires keeping the route's data currently in use and the overhead that enters the network. ZRP, DDR and DST [11] are samples of Hybrid routing protocols.

III.II. POSITION-BASED ROUTING PROTOCOLS

position-based routing protocols delete some of the limitations of topology-based routing method by using extra data. These routing protocols require data on physical position of existing nodes. Usually, each node or positions are gained by GPS or some other position services [12, 13].

In position-based routing protocols, the sender of a packet finds the position of destination by using location service and they mention it in the address section of packet and then they send it by use of desired packet routing algorithms and in each packet this position and the position of neighboring nodes are mentioned.

Thus, position-based routing does not require settlement or maintaining routes. The nodes neither save routing tables nor they transmit messages for updating routing tables. Position-based routing use Location Service and Forwarding Strategy combinations in this way that at first they determine the destination position by Location Service and then Forwarding Strategy is used for sending the package.

III.II.I. LOCATION SERVICE

In position-based routing, before a packet being sent, it needs to determine the position of its destination. Location Services are categorized based on this fact that what number of nodes are server (specified number of nodes or all of them). Therefore, each Location Service may keep the position of specified number of nodes or the position of all existing nodes in the network. Four combinations of (Some-For-All) SFA, (Some-For-Some) SFS, (All-For-Some) AFS and (All-For-All) AFA are discussed in Location Service.

In position-based routing, forwarding decision by a node is settled by a node based on position of destination and the position of its neighbors connected as On-hop. And the destination's position is mentioned in the packet's header.

Normally, the data on position of neighbors is gained by On-hop broadcast. This is done periodically by all nodes to update the nodes' position periodically.

III.II.II. FORWARDING STRATEGY

Three packet forwarding strategies are used in position-based routing included of Greedy Forwarding, Restricted Directional Flooding and Hierarchical Approaches. In the first strategy, a node sends the given packet for an On-hop neighbor. In the

second strategy, a node sends the given packet for more than an On-hop neighbor. That in both strategies this neighbor is located nearer than the node itself for sending the pack to the destination. Selection of neighbor in Greedy strategy depends on algorithm's criteria. It is apparently obvious that both packet forwarding strategies may vanish, because it is possible for a state in which an On-hop neighbor does not exist to be closer to destination than the sending node. A recovery strategy removes such defections.

The 3rd forwarding strategy is Hierarchy form which can be developed for a large number of mobile nodes. As an example of Hierarchical routing we can mention to two following strategies: Greedy forwarding for wide area routing and Non-position-based approaches

IV. SECURITY IN MANET SYSTEMS

Determining reliability is an applied subject in MANET systems, because in architecture of a MANET system, since no network structure is fixed and defined, a mobile node in this network sends the data packets to destination as fig. 1 directly or via neighboring nodes. But, this position requires security considerations, because these security nodes cannot always be trusted, because some of the mean users can eavesdrop in the route or data packet routing area or create traffic and result in Denial of Service (DOS) [14].

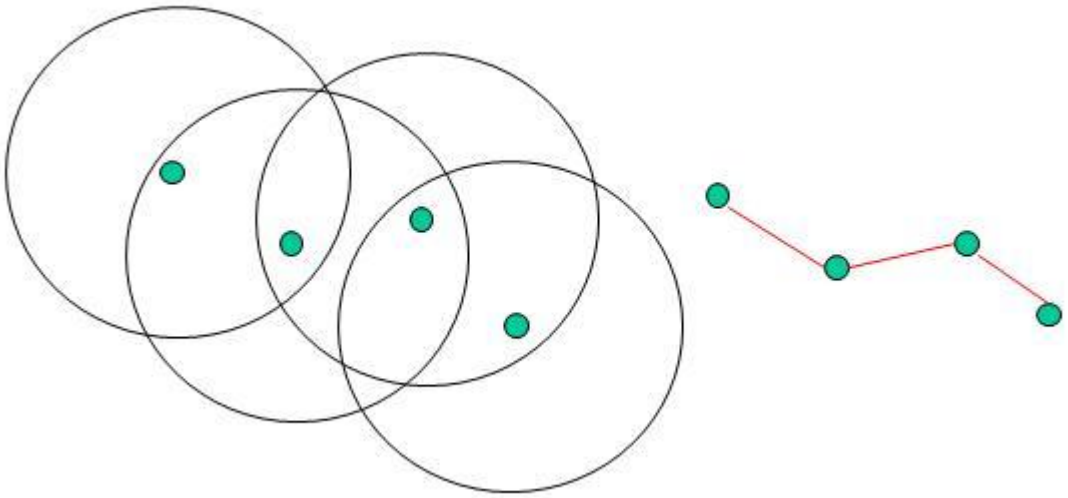

Figure 1. Transmission method for data packets in network [15]

Despite communication via internet, traditional security mechanisms such as reliability determining protocols and data coding techniques cannot easily adjust on Ad Hoc network, because no official structure of certification or key distribution exists in this network. This issue strictly stands against other mobile networks such as Mobile IP or cell phones in which the nodes are always under supervision of management.

Based on the specifications of this network, dividing neighboring nodes in two groups of secure and insecure is very critical. Generally, security considerations in MANET systems do not belong to an individual, but is related to a group of nodes like a company or project. On the other word, getting prepared against security threats in a MANET is done based on distinguishes of legal group members which are completed in the first step.

When reliability determining for group members in a MANET is completed, the next phase is to protect the relation between the group members themselves, because in reliability determining protocols, two issue of reliability determining and data comprehensiveness cannot be separated. Because, in a relation it is not just enough for the communication parties to know whether the message is came from a legal member and they are not sure if it has changed in the path illegally or inversely they make sure that the message is not illegally changed, but they don't know from whom the message is came. Using a common key for coding and decoding messages can respond to this need for data comprehensiveness. But what is more important and complicated here is management and key distribution of group that some issues shall be observed in this regard:

- Legal members shall be able to gain the group key in a crowded network that network's topology and mobile nodes change dynamically.
- Even if a message was eavesdropped between a new member and other nodes, the group key shall not be revealed for members.

Based on these observations, in a reliability determining protocol, group members are presented based on the knowledge in MANET without a structure that includes two phases of reliability determining structure of group members and secrete group key. By termination of these two phases, confirmed members have received a secret key and can make a secure connection with other legal group members.

As it was said, this protocol is composed of two phases. In the first phase which has the duty of reliability determining, Zero Knowledge Proof is used and in the second phase that manages the secret group key, uses Threshold Cryptography for creating secure connection between group members and data comprehensiveness.

V. CONCLUSION

In this paper, mobile Ad Hoc networks were introduced and it was said that these networks have no fix and predefined structure. Nodes are free to move and nodes' position, network's topology and method of connections are dynamically changing. However, these properties provide security challenges for networks that one of the most important one is making reliability determining methods in order to access data, resources and data comprehensiveness. Since the connection is made by neighboring nodes and these nodes are not always reliable, this issue is very critical. By taking to account the special properties of these networks, traditional security mechanisms cannot be applied in them.

REFERENCES

[1] James A. Freebrersyser , Barry Leiner A DOD perspective on mobile ad hoc Networks In : chales E. parkins(Ed.), Ad hoc Networking, Addison Wesley, Reading MA, pp29-51

[2] W. Fifer,F.Bruno The Low-cost Packet Radio Proceedings of the IEEE , pp 33-42

[3] B. Leiner, R. Ruth, A.R.Sastry Goals and challenges of the DARPA Glomo Program IEEE Personal Communications , pp 34-43

[4] IEEE Standard for Wireless LAN-Medium Access Control and Physical Layer Specification P802.11

[5] D. Beyer , M. D. Vestrich, and J. J. Garcia-Luna-Aceves The Rooftop Network : Free , High-Speed Network Access For Communities , Hurley Community and Keller , Edrs., The First 100 : New Options For Internet and Broadband Access, MIT Press , pp75-91.

[6] C. perkins and P.Bhagwat Highly Dynamic Destination Sequenced vector Routing (dsdv) for Mobile Computers Comp. Commun. Rev. Distance Oct. pp 234-44.

[7] P.Jacquet et al Optimized Link State Routing Protocol. Internet draft, manet – olsr-04.

[8] B. Bellur , R. Ogier , and F. Templin Topology Broadcast Based on Forwarding (tbrpf), Internet draft, draft-ietf-manet-tbrpf-01. Txt, Revers-Path work in progress .

[9] D. Johnson and D. Maltz Mobile Computinng, Chap. 5- Dynamic SourceRouting, Kluwer Academic Publishers , pp 153-81.

[10] V.Park and M. Corson A Highly Adaptive Distributed Routing Algorithm for Mobile Wireless Networks Proc. INFOCOM '.

[11] C.Perkins and E. Rover Ad-hoc on- demand Distance Vector Routing Proc.2nd IEEE Wksp. Mobile Comp. Sys.App, feb. pp 90-100.

[12] JBroch et al A Performance Comparison of Multi-hop Wireless Ad HocNetwork Routing Protocols Proc.4 th ACM/IEEE Int'l.Conf. Mobile and Networking MOBICOM '98, Dallas , TX, USA , PP 85- 97.

[13] E. Kaplan Understanding GPS , Artech House .

[14] Asaeda, Hitoshi, Rahman, Musfiq, Manshaei, Mohammad Hossein, Fukuzawa, Yasuko, Implementation of Group Member Authentication Protocol in Mobile Ad-hoc Networks

[15] Iyer, Sridhar, Mobile Ad Hoc Networks, http://www.it.iitb.ac.in/~sri/talks/manet.ppt, last visited: December ,2012