International Journal of Advances in Engineering Research http://www.ijaer.com

(IJAER) 2013, Vol. No. 3, Issue No. IV, April **ISSN: 2231-5152**

AUTHENTICATED DATA TRANSMISSION IN DECENTRALIZED WIRELESS MOBILE AD-HOC NETWORK (MANET)

Mr. Vishal Rajput [#1]

[#] *Assistant Professor, Narmada College of Computer Application, MCA Department, Bharuch, India*

[1]*vish_raj9374@yahoo.com*,

ABSTRACT

In this paper we discuss regarding authentication for secure data transfer in mobile Ad hoc network. Owe to the vulnerable nature of the mobile ad hoc network, there are number of security threats that disturb the development of this algorithm to secure data transfer in MANAT. We first analyze the main vulnerabilities in the mobile ad hoc network, which have made it much easier to suffer from attacks than the traditional wired network. Then I discuss the various security criteria of the current security solutions for the mobile ad hoc network. Also define the proposed authentication model for data transfer in Mobile Ad Hoc network. With the increasing interest in MANET, there has been a greater focus on the subject of authenticated communication on such networks. Out of the many discussions and research groups discussing the different security issues in the field of MANAT, many papers have been written describing different proposed secure routing protocols that defend against malicious nodes' attacks that MANETs face. However, the majority of these MANET secure routing protocols did not provide a complete solution for all the MANETs' attacks and assumed that any node participating in the MANET is not selfish and it will cooperate to support different network functionalities.

The authenticated routing for ad hoc networks secure routing protocol was chosen for analysis. My research strategy is to choose one of the authenticated routing protocols according to its security-effectiveness, study it and analyze its functionality and performance. The authenticated routing for ad hoc networks secure routing protocol was chosen for analysis. Then, the different existing cooperation enforcement schemes were surveyed so that to come up with a reputation-based scheme to integrate with the adhoc routing central topology. In this paper we provide specific proposed solution against the different attacks in adhoc network.

Keywords: *Mobile Ad Hoc Network; Routing protocols; Classification of protocols; Security issues;*

INTRODUCTION

In ad hoc networks every communication terminal or radio terminal RT communicates with its partner to perform peer to peer communication. In ad hoc networks all the communication network protocols should be distributed throughout the communication terminals .Mobile Adhoc Network

is a collection of independent mobile nodes that can communicate to each other via radio waves. The connected mobile nodes that are in radio range of each other can directly communicate, whereas others needs the aid of intermediate nodes to route their packets. . If the required RT is not a neighbor to the initiated call RT (outside the coverage area of the RT), then the other intermediate RTs are used to perform the communication link. This is called multi hope peer to peer communication. This collaboration between the RT is very important in the ad hoc networks. These networks are fully distributed network, and can work at any place without the help of any infrastructure. This property makes these networks highly flexible and more robustness.

The characteristics of these networks are as follows:

- Nodes can perform the roles of both hosts and router.
- No centralized controller and infrastructure. Intrinsic mutual trust.
- Energy constraints & Limited security in network.
- Autonomous, no infrastructure needed for communication setup.

Generally, the communication terminals have an mobility nature which makes the topology of the distributed networks time varying. The dynamic nature of the network topology increases the challenges of the design of ad hoc networks. Each RT is usually powered by energy limited power source (as rechargeable batteries).here we discuss indirect effect of routing into the power consumption. The power consumption of each radio terminal could be divided generally into three parts, power consumption for data processing, power consumption to transmit its own information to the destination, and finally the power consumption when the RT is used as a router, i.e. forwarding the information to another RT in the network. The energy consumption is a critical issue in the design of the ad hoc networks.
The mobile devices usually have limited storage and low computational capabilities. They heavily depend on other hosts and resources for data access and information processing. A reliable network topology must be assured through efficient and secure routing protocols for Ad Hoc networks.

Security has become a primary concern in order to provide protected communication between mobile nodes in a hostile environment and the ultimate goal of the security solutions for MANETs is to provide security services such as Confidentiality, Integrity, Availability, Non-Repudiation and Authentication, Authorization and Anonymity. Confidentiality ensures that Secret information or data is never disclosed to unauthorized devices. Integrity tells that a received message is not corrupted. Availability permits the survivability of network services despite Denial-of-Service attacks. Non-repudiation ensures that the sender of a message cannot deny having sent the message.

Authentication enables a node to ensure the identity of the Peer node it is communicating with. Authorization is a process in which an entity is issued a credential, which specifies the privileges and permissions it has and cannot be falsified, by the certificate authority.

From the above discussion we found that the most of the attacks in the MANET is formed during the routing mistakes or from the authentication and un-authorization gaps. in the next section we discuss the problem that are responsible for forming these attacks.

ROUTING IN MOBILE AD-HOC NETWORKS

1. Proactive/Reactive Ad Hoc Routing Protocols

The existing ad hoc routing protocols can be broadly classified into the following two categories:

Proactive protocols (e.g. WRP or wireless routing protocol): by broadcasting control packets containing routing table information (e.g. distance vector), these protocols attempt to maintain at all time up-to-date routing information from each node to every node.

Reactive protocols (e.g. AODV or Ad hoc on-demand distance vector routing): only when a route to destination is required, a node initiates a route discovery process. Once a route has been established, it is maintained by a route maintenance procedure until the route is no longer desired. Unfortunately, these protocols suffer from a number of shortcomings: scalability problems with growing network size and their performance is only optimal under certain network conditions (mobility, network load, network topology).

In any network infrastructure the routing algorithms and routing strategy provide the key or main role. Here we discuss some routing protocols and the infrastructures gap that is responsible for these attacks.

AODV (Ad-hoc on-demand distance vector routing)

This protocol is frequently used in the MANET network design and analysis of the performance of the system. The major gap in this protocol it is not updatable and at the time of requirement this protocol is active and makes effort for route discovery. During this it can be adopt or automatically join the malicious node.

DSDV (Destination-Sequenced Distance Vector routing)

The advance version of this routing protocol is used as the AODV. this routing is a table driven routing protocol in this protocol system keep the routing and path information from all time and it is updated at each route discover. But due to mobility sometimes this is fails to provide the correct information and again route discovery is performed.

In the above section we can see both kinds of routing algorithms table driven and without table driven routing protocols. The main problems are listed below:

- In on demand routing strategy we can save battery power and energy consumption during the data transfer but we can easily join the malicious nodes in the network.

- In on demand routing when required than a path is discovered thus it is good for links which is brake during its mobility model.

In the above discussion we have found the different routing algorithm for communication in mobile Ad-hoc network in which we have discuss regarding DSDV algorithm in which it will create a path table from source to destination. Let us see on next point how Mobile Ad-hoc network find a specific path for sending a data into wireless network

ROUTING PATH IMPLEMENTATION BACKGROUD

There are presently no lightpath network implementations on PCs. Therefore, we implemented a program which run lightpath network control plane. The GMPLS (Generalized Multiprotocols Label Switching) achieves a label switching network on multi–protocols. A label has information on link attributes that includes the switching capabilities of packets, fibers, wavelength lambdas, and TDM (Time Division Multiplexing) time slots. Using the assigned labels, the network nodes switch the input interface bound to a lambda ('photonic switching,' or 'wavelength Switching) to an output interface bound to a lambda. The processing layers for path establishment in this GMPLS architecture follow the description in Figure On receiving a path establishment request; the routing plane selects the proper route for the request. The resource reservation plane then signals the reservation process to neighboring nodes along the control channel.

The RSVP (Resource Reservation Protocol) protocol leads the route information to the RSVP path message, which goes to the control channel through within an explicit route. On receiving the RSVP path message, the intermediate node confirms the path message's label information on whether it has the capabilities for the specified link or not and if it is capable of resource reservation then forwards this to the next node. On receiving the path message, the receiver node confirms the path message and returns the RSVP reserve message to the sender node with reservation and switching the label of the interfaces among the routes.

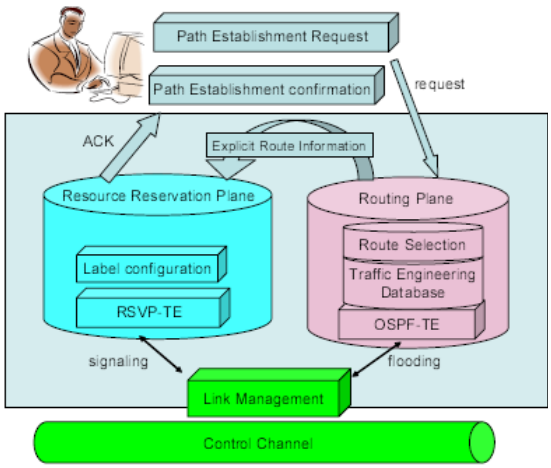

Fig 1: Signaling Architecture and its control plan

The routing plane has the OSPF–TE signaling protocol, the Traffic Engineering database, and a routing algorithm. The OSPF–TE protocol floods information on attributes of links between neighboring nodes. The Traffic Engineering database collects the flooded OSPF data packets. Routing algorithm uses the information from Traffic Engineering database, and selects a suitable route. Link Management manages the control channel, which provides fault discovery (e.g., link disconnection, node failure, and data transmission degradation). The control plane's signals are protected from any faults by the link management protocol.

SECURITY THREATS IN MOBILE AD-HOC NETWORK

Security is an important thing for all kinds of networks including the Wireless Ad Hoc Networks. It is obviously to see that the security issues for Wireless Ad Hoc Networks are difficult than the ones for fixed networks.

This is due to system constraints in mobile devices as well as frequent topology changes in the Wireless networks. Here, system constraints include low-power, small memory and bandwidth, and low battery power.

Mobility of relaying nodes and the fragility or routes turn Wireless Ad-hoc Network architecture into highly hazardous architectures. No entity is ensured to be present at every time and it is then impossible to rely on a centralized architecture that could realize network structure or even authentication. The people who consider the Mobile Ad hoc Networks are not a flawed architecture, while we cannot see it used in practice is only because most of its applications are in military are totally wrong. It is true that Mobile Ad hoc Networks come from the military. But perhaps those persons forgot one of the most important things: the Security!

Everybody knows that the core requirement for military applications dealing with trust and security! That is to say, security is the most important issue for ad hoc networks, especially for those security sensitive applications. As we have mentioned before, in Mobile Ad-hoc Networks, security is difficult to implement because of the networks constrains and the rapidly topology changes. After investigation, we found that lake of security threats related problems in the Mobile Ad-hoc Networks.

Security Services: If we are taking about security of information then following services come in mind.

- Confidentiality (privacy)
- Authentication (who created or sent the data)
- Integrity (has not been altered)
- Non-repudiation (the order is final)
- Access control (prevent misuse of resources)
- Availability (permanence, non-erasure)

Let us see the proposed conversion algorithm of the Mobile Ad Hoc Networks. In this algorithm I transfer packet through the proper destination using finding a perfect access point of the destination. This perfection is made by the centralized system.

1. Proposed algorithm for MANAT

- Designing System design needed to implement the idea of this proposal
  (The Monitoring in Optimum Routing Algorithm.), and achieve the following goals:
  - Less congestion control, overhead control and communication cost.
  - High speed during route discovery, update and data maintenance.
  - Packets transfer guarantee and insurance.
  - Optimum bandwidth for data packet transmission.
  - Also providing a secure data transfer using proper monitoring between source nodes to destination node.

As per the above discussion of different protocol here I design some basic point in which I studies the different protocol and try to utilize this for secure network for large scale wireless network which is mostly used in defense for transferring secure information into same network. Related points are as follows:

Table 1 Network Layer Threats and Countermeasures

Threats	Countermeasure
Wormhole	Physical monitoring of Field devices and regular monitoring of network using Source Routing. Monitoring system may use Packet Leach techniques.
Selective forwarding	Regular network monitoring using Source Routing
DoS	Protection of network specific data like Network ID etc. Physical protection and inspection of network.
Sybil	Resetting of devices and changing of session keys.
Traffic Analysis	Sending of dummy packet in quite hours; and regular monitoring WSN network.

In the above table i described different attack in wireless network due to this reason here I proposed solutions to overcome from this problem design different modules are:

- We proposed **model** for MANET based on DV,AODV
- Number of Optimum Routes depends on the Number of neighbours where Maximum Number from each neighbour.
- Low overhead and faster than the standard protocols.
- Maintain table driven information of each node in one of the central system in to the same network.
- Topology to maintain registration of each node information into the table.
- Required registration before sending any message or file into the network.
- Node should get **Information** from any route pass through it and update in central system database.
- Main system continues send hello message to verify neighbor node is connected or not if it is not connected then delete node information into the table.
- If any node do any malicious activity into the network then system automatically delete its related information into the network.

CONCLUSION AND FUTURE ENHANCEMENT

This paper provides a comprehensive analysis of the most recently proposed multipath routing protocols for wireless sensor networks. Nowadays, multipath routing techniques are considered an efficient approach to improve network capacity and resource utilization under heavy traffic conditions. With respect to the recent advances in the development of multipath routing protocols for wireless sensor networks, there is a need to investigate the significance as well as the detailed operation and classification of the proposed approaches. To fill this gap, in this paper we have attempted to identify the challenges pertaining to the design of multipath routing protocols for wireless sensor networks. In addition, we have highlighted the main advantages of using multipath routing approach to satisfy the performance requirements of different applications. This paper also introduces a new taxonomy on the multipath routing protocols designed for wireless sensor networks. The provided classification is performed based on the employed path utilization methods that can be used by multipath routing protocols to achieve various performance benefits.

REFERENCES

[1] Yan Wang and Ming Hu "Timing evaluation of the known cryptographic algorithms "2009 International Conference on Computational Intelligence and Security 978-0-7695-3931-7/09 $26.00 © 2009 IEEE DOI 10.1109/CIS.2009.81.

[2] International Journal of Advanced Research in Computer Science and Software Engineering, Volume 2, Issue 1, January 2012 ISSN: 2277 128X.

[3] Symmetric key cryptography using random key generator, A.Nath, S.Ghosh, M.A.Mallik, Proceedings of International conference on SAM-2010 held at Las Vegas(USA) 12-15 July,2010, Vol-2,P-239-244.

[4] Data Hiding and Retrieval, A.Nath, S.Das, A.Chakrabarti, Proceedings of IEEE International conference on Computer Intelligence and Computer Network held at Bhopal from 26-28 Nov, 2010.

[5] Text book William Stallings, Data and Computer Communications, 6eWilliam 6e 2005.

[6] Md. Nazrul Islam, Md. Monir Hossain Mia, Muhammad F. I. Chowdhury, M.A. Matin "Effect of Security Increment to Symmetric Data Encryption through AES Methodology" Ninth ACIS International Conference on Software Engineering, Artificial Intelligence, Networking, and Parallel/Distributed Computing 978-0-7695-3263-9/08 DOI 10.1109/SNPD.2008.101 IEEE 2008.

[7] C.E.Perkins and E.M. Royor," Ad hoc on demand distance vector routing.", In IEEE WMCSA'99.

[8] David B. Johnson, "Routing in Ad Hoc Networks of Mobile Hosts", Proceedings of the IEEE Workshop on Mobile Computing Systems and Applications, December 1994.

[9] Akkaya, K.; Younis, M. A Survey on Routing Protocols for Wireless Sensor Networks. Ad Hoc Netw. J. 2005, 3, 325-49