https://dx.doi.org/10.24001/ijaems.3.5.19 *ISSN: 2454-1311*

Proposed Scheme for Secured Routing in MANET

Nidhi Goyal, Susheel Kumar

Dept. of Computer Science, Samalkha Group of Institutions, Samalkha (HR.), Kurukshetra University, Kurukshetra, India

Abstract— *A Mobile Adhoc Network (MANET) is characterized by mobile nodes, multihop wireless connectivity, infrastructure less environment and dynamic topology. A recent trend in Ad Hoc network routing is the reactive on-demand philosophy where routes are established only when required. Stable Routing, Security and Power efficiency are the major concerns in this field. This paper is an effort to study security problems associated with MANETS and solutions to achieve more reliable routing. The ad hoc environment is accessible to both legitimate network users and malicious attackers. The study will help in making protocol more robust against attacks to achieve stable routing in routing protocols.*

Keywords— Ad hoc Networks, AODV, security, wireless network, packet delivery.

I. INTRODUCTION

Since their emergence in the 1970s, wireless networks [1, 11] have become increasingly popular in the computing industry. This is particularly true within the past decade, which has seen wireless networks being adapted to enable mobility. Wireless networks are emerging fast as latest technology to allow users to access information and services via electronic media, without taking geographic position in account. Mobile hosts and wireless networking hardware are becoming widely available, and extensive work has been done recently in integrating these elements into traditional networks such as the Internet. Wireless networks have taken the world by storm. Enterprises and homeowners are avoiding the expenses and delays associated with installing wired networks. High-speed Internet facility is enjoyed by travelers all over the places worldwide. Along with increases in throughput, wireless networks remain unlicensed and affordable. This has further helped their exponential growth in businesses, homes, communities and open spaces. There are currently two variations of mobile wireless networks: Infrastructured or Infrastructure less. [10, 12, 13]. In Infrastructured wireless networks, the mobile node can move while communicating, the base stations are fixed and as the node goes out of the range of a base station, it gets into the range of another base station that is within its communication radius. The figure 1, given below, depicts the Infrastructured wireless network. Typical applications of this type of network include office wireless local area networks (WLANs). In Infrastructureless wireless network commonly known as an ad hoc network, the mobile node can move while communicating, there are no fixed base stations and all the nodes in the network act as routers. The mobile nodes in the Ad Hoc network dynamically establish routing among themselves to form their own network 'on the fly'. This type of network can be shown as in figure 2.

II. AD HOC NETWORK

An Ad hoc network [1, 11] is a self-configuring network of wireless links connecting mobile nodes. These nodes may be routers and/or hosts. Each node or mobile device is equipped with a transmitter and receiver. They are said to be purpose-specific, autonomous and dynamic. Ad hoc networking is a concept in computer communications, which means that users wanting to communicate with each other form a temporary network, without any form of central administration. Term Ad hoc means a network which can take different forms in terms of topologies and in term of devices used. Ad hoc devices can be mobile, standalone or networked.

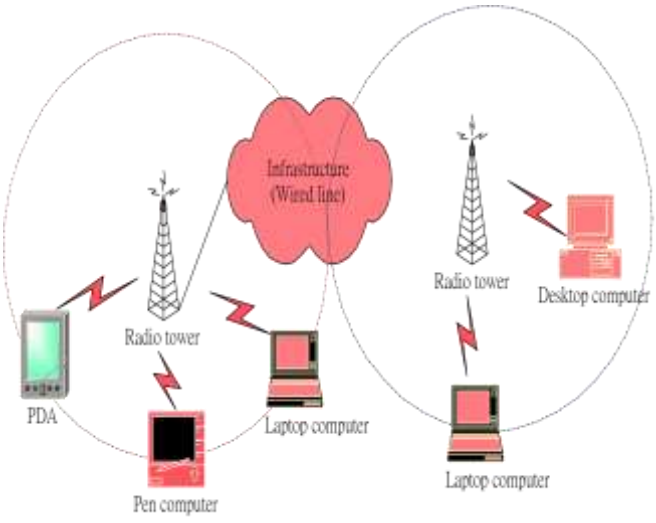

Fig.1: Infrastructured Wireless Networks

https://dx.doi.org/10.24001/ijaems.3.5.19 *ISSN: 2454-1311*

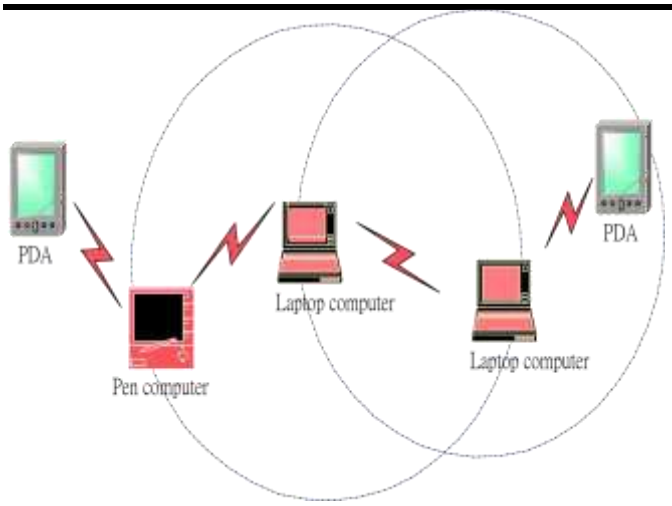

Fig.2: Infrastructure less or Ad Hoc Wireless Network

"A Mobile Ad hoc Network (MANET) [4, 5] is an autonomous system of mobile hosts which are free to move around randomly and organize themselves arbitrarily" or we can say that "It is a collection of wireless mobile nodes forming a temporary/short-lived network without any fixed infrastructure where all nodes are free to move about arbitrarily and where all the nodes configure themselves". In MANET, each node acts both as a router and as a host & even the topology of network may also change rapidly. MANET is viewed as suitable systems which can support some specific applications as virtual classrooms, military communications, emergency search and rescue operations, data acquisition in hostile environments, communications set up in Exhibitions, conferences and meetings, in battle field among soldiers to coordinate defense or attack, at airport terminals for workers to share files etc. In Ad hoc networks nodes can change position quite frequently. The nodes in an ad hoc network can be Laptops, PDA (personal digital Assistant) or palm tops etc. These are often limited in resources such as CPU capacity, storage capacity, Battery Power, Bandwidth. Each node participating in the network acts both as a router and as a host and must therefore be willing to transfer packets to other nodes. For this purpose a routing protocol is needed and the new protocol should try to minimize control traffic. An ad hoc network has certain characteristics, which impose new demands on routing protocols. The most important characteristic is dynamic topology, which is a consequence of node mobility. It should be reactive i.e. calculates routes only upon receiving a specific request.

The Internet Engineering Task Force currently has a working group named Mobile Ad hoc Networks (MANET) that is working on routing specifications for Ad hoc networks. This research work will evaluate some of the existing protocols and suggests a new protocol. To accomplish this task, several routing protocols for Ad hoc networks have been studied such as Dynamic Source Routing (DSR)[6], Dynamic Distributed Routing (DDR)[7], Temporarily Ordered Routing Algorithm (TORA)[2], Ad Hoc On Demand Distance Vector Routing (AODV)[4,5]. In all the protocols major emphasis has been on stable and shortest routes ignoring the major issue of delay in response whenever break occurs. Most of the protocols proposed require knowledge of the network topology for routing. These protocols involve communication overheads of route discovery and maintenance. Later, position based protocols were proposed to eliminate these overheads. Most of the protocols in this category, however, use single route and do not utilize multiple alternate paths. Those routing protocols should also minimize the usage of valuable resources such as bandwidth, power and processor.

III. MANET CHALLENGES

The special features of mobile ad hoc networks bring great technological opportunities together with different challenges[9,10]. Some of the key challenges in the area of mobile ad hoc networks include:

1. Unicast routing
2. Multicast routing
3. Dynamic network topology
4. Speed
5. Frequency of updates or Network overhead
6. Scalability
7. Mobile agent based routing
8. Secure routing
9. Quality of Service
10. Energy efficient/Power aware routing

The key challenges faced at different layers of MANET are shown in figure 3. It represents layered structure and approach to ad hoc networks.

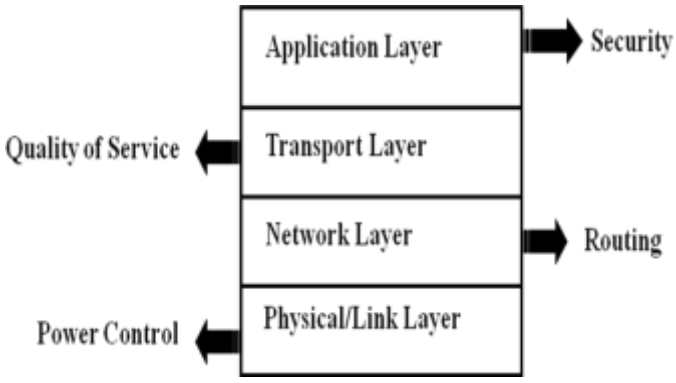

Fig.3: Challenges at different layers of MANET

https://dx.doi.org/10.24001/ijaems.3.5.19 *ISSN: 2454-1311*

IV. SECURITY ISSUE OVER AD HOC NETWORKS

Many organizations including retail stores, hospitals, airports and business enterprises plan to capitalize on the benefits of "going wireless". But if we think about the security of the modern wireless network, this wouldn't looks so positive. There have been numerous published reports and papers describing attacks on wireless networks that expose organizations to security risks such as attacks on confidentiality, integrity, non repudiation and network availability [8,9]. There are several proposals to solve these issues but they target specific threats separately. Therefore, there is a requirement to have an efficient security system which takes care of all aspects of security.

Security Threats: Network security attacks are typically divided into passive & active attacks[ ]as shown in table 1.

Passive Attack: An attack in which an unauthorized party gains access to an asset and does not modify its content. Passive attacks can be either eavesdropping or traffic analysis (sometimes called traffic flow analysis). These two passive attacks are described below.

- **Eavesdropping:** The attacker monitors transmissions for message content. An example of this attack is a person listening into the transmissions on a network topology between two workstations or tuning into transmissions between a wireless handset and a base station.
- **Traffic analysis:** The attacker, in a more subtle way, gains intelligence by monitoring the transmissions for patterns of communication. A considerable amount of information is contained in the flow of messages between communicating parties.

Table 1: Passive vs. active attacks

Passive attacks	Eavesdropping, traffic analysis
Active attacks	Masquerading/Spoofing, Replaying, Message modification, DoS

Active Attack: An attack whereby an unauthorized party makes modifications to a message, data stream, or file. It is possible to detect this type of attack but it may not be preventable. Active attacks may take the form of one of four types masquerading, replay, message modification, and Denial-of-Service (DoS). These attacks are summarized as:

- **Masquerading:** The attacker impersonates an authorized user and thereby gains certain unauthorized privileges. A spoofing attack is a situation in which one person or program successfully masquerades as another by falsifying data and thereby gaining an illegitimate advantage.
- **Replay:** The attacker monitors transmissions and retransmits messages as the legitimate user.
- **Message modification:** The attacker alters a legitimate message by deleting, adding to, changing, or reordering it.
- **Denial-of-Service:** The attacker prevents or prohibits the normal use or management of communications facilities.

The consequences of these attacks include, but are not limited to, loss of proprietary information, legal and recovery costs, tarnished image, and loss of network service.

Due to the dynamically changing topology and infrastructure less, decentralized characteristics, security is hard to achieve in mobile ad hoc networks. Hence, security mechanisms have to be a built-in feature for all sorts of ad hoc network based applications.

V. EXISTING SECURITY MEASURES

Some of the measures that can be incorporated are:

1. **Virtual Private Networks (VPN):** This offers a solid solution to many security issues, where an authenticated key provides confidentiality and integrity for IP (Internet Protocol) data grams. Software are available to implement VPNs on just about every platform. Authentication depends upon three factors such as password, fingerprints and a security token.
2. **Encryption:** Encryption is a technique used for many years for passing information from one place to other in a secured manner. A message in its original shape is referred to as a plaintext (or Text) and a message used to conceal original message is called Ciphertext (or Cipher). The process of changing plaintext into ciphertext is called Encryption and the reverse process is called decryption. There are many algorithms available for these processes. Some of them are Data Encryption Standard (DES), International Data Encryption algorithm (IDEA) and Public key algorithm (RSA). These algorithms are key based algorithms.
3. **One Way Hash Function**: There is another algorithm called one way hash Function. It is like checksum of a block of text and is secure. It is impossible to generate the same hash function value without knowing the correct algorithm and key. It accepts a variable size message and produces an affixed size tag as output.
4. **Digital Signature**: A digital signature is an electronic signature that can be used to authenticate the

https://dx.doi.org/10.24001/ijaems.3.5.19 *ISSN: 2454-1311*

identity of the sender or the signer of a message/document, and possibly to ensure that the original content of the message or document that has been sent is unchanged. Digital signatures are easily transportable, cannot be imitated by someone else, and can be automatically time-stamped. External attacks can be checked using Confidentiality of the routing information and also by authentication and integrity assurance features. Encryption can be solution to this. Digital signature can be applied.

VI. PROPOSED SCHEME

The effort is to propose a solution for routing in Ad hoc networks by tackling the core issue of stability and security. A protocol will be developed which improves existing on-demand routing protocols by adding security parameter. An effort will also be made to develop a cryptographic algorithm or to implement new strategy to existing algorithm.

The scheme will establish multi paths without transmitting any extra control message. It will offer quick adaptation to distributed processing, dynamic linking, low processing and memory overhead and loop freedom at all times. The proposed scheme will respond to link breakages and changes in network topology in a timely manner. The distinguishing feature will be security factor for Ad hoc routing protocol. The work will present a new scheme based on stable and secured nodes and the goal is to able to address the following features:

- The proposed scheme performs better for finding a good route, such that better packet delivery is assured.
- The scheme performs well in denser mediums.
- Scheme should be successful in minimum hop count as metrics for optimality.
- The Scheme should offer Secured Routing
- It should be able to provide stable route selection.
- The Proposed scheme should perform with both bi-directional and uni-directional traffic patterns.

The Metrics[1,3,12] that will be used for Performance evaluation and comparison will be:

- **Packet Delivery Ratio**: The fraction of successfully received packets, which survive while finding their destination is called packet delivery ratio. This performance measure also determines the completeness and correctness of the routing protocol.
- **End-to-End Delay**: Average end-to-end delay is the delay experienced by the successfully delivered packets in reaching their destinations. This is a good metric for comparing protocols. This denotes how efficient the underlying routing algorithm is, because delay primarily depends on optimality of path chosen.
- **Throughput:** This declares overall throughput in terms of packets received and helps in performance evaluation of the proposed scheme.

Proposed Scheme

Hashing is done for route request, reply and local route repair and not in route error and route erasure phases so that less overhead occurs. If in REQ phase if intermediate node cannot satisfy the security and power requirements, the REQ packet is dropped and not forwarded. Arrival of REQ to Destination will ensure a safe path. REP packet contains this security information specified by sender. So additional field is added to REQ and REP packet formats.

1 Source node broadcasts routing request message to its neighbors in order to find a route to destination node.

2. The neighbors of the source node forward the request to their neighbors if the security evaluation on the source node pass its predefined threshold, and so on, until either the destination or an intermediate node with a "fresh enough" route to the destination is reached.

3. If some nodes respond that they have fresh enough route to the destination node,, Based on the evaluation result and hops of the routes, the source node selects one preferred route, which it believes the best.

4. After receiving the data packages, the destination node applies the same method above to reply the confirmation message if the source node requests it. It is not mandatory to use the same route as the source for better security consideration.

5. If within the time slot, the destination's confirmation arrives and can be verified as valid, the source node will continue sending data packages via the underlying route. If the destination's confirmation cannot receive within the preferred time slot, the source node will update its route table and go for local repair.

6. The source node selects the second best route.

VII. CONCLUSION

The existing routing protocols are typically attack-oriented. They first identify the security threats and then enhance the existing protocol to conquer such attacks. The ultimate goal for adhoc network security is to develop a multifold security solution that results in in-depth protection that offers multiple lines of defense against both known and unknown security threats. The objective in this study is to find a multifold security solution by developing a new on-demand

https://dx.doi.org/10.24001/ijaems.3.5.19 *ISSN: 2454-1311*

stable and secure routing protocol. The work will help in development of new protocol and standardize the existing schemes.

ACKNOWLEDGEMENT

We sincerely wish to thank Dr Ashwani Kush, Head, Dept of computer science, UCK for his valuable help and kind advice.

REFERENCES

[1] A. Kush, P. Gupta, R. Kumar; Performance Comparison of Wireless Routing Protocols; Journal of CSI, Vol. 35 No.2, April-June 2005.

[2] A.Kush, P.Gupta , C J Hwang **"**Stable and Energy Efficient Routing for Mobile Adhoc Networks" Information Technology: New Generations, 2008. ITNG 2008. Fifth International Conference, LAS VEGAS USA 7-9 April 2008 Page(s):1028 – 1033 Digital Object Identifier 10.1109/ITNG.2008.230 at IEEE explore.

[3] Bayya, Arun. "Security in Ad hoc Networks", Computer Science Department. University of Kentucky.

[4] C.Parkins and E.Royer , "Ad Hoc on demand distance vector routing", 2nd IEEE workshop on mobile computing , pages 90-100, 1999.

[5] Charles Perkins, Elizabeth Royer, Samir Das, Mahesh Marina, "Performance of two on-demand Routing Protocols for Ad-hoc Networks", IEEE Personal Communications, February 2001, pages 16-28.

[6] D.B.Johnson and D.A. Maltz, "Dynamic source routing in ad hoc networks", Kluwer academic publishers, 1996.

[7] D. B. Johnson, D. A. Maltz, Y.C. Hu, "The Dynamic Source Routing Protocol for Mobile Ad Hoc Networks (DSR)", IETF Draft, April 2003, work in progress. http://www.ietf.org/internet-drafts/draft-ietf-manet-dsr-09.txt.

[8] D. B. J., Yih-Chun Hu, Adrian Perrig, "Ariadne: A secure on-demand routing protocol for ad-hoc networks", Proceedings of the Eighth Annual International Conference on Mobile Computing and Networking (MobiCom 2002), Sept. 2002.

[9] Hao Yang, Haiyun Luo et al., 'Security in Mobile Ad Hoc Networks: Challenges and Solutions", UCLA Computer Science Department.

[10] Md. Golam Kaosar, Hafiz M. Asif, Tarek R. Sheltami, Ashraf S. Hasan Mahmoud, "Simulation-Based Comparative Study of On Demand Routing Protocols for MANET", available at http://www.lancs.ac.uk.

[11] NIST, Fed. Inf. Proc. Standards, "Secure Hash Standard," Pub. 180, May 1993.

[12] A.Kush , Sunil Taneja, " simulation of MANET schemes",in International Journal of Computing and Business Research IJCBR, Vol 1, Issue 2, Nov, 2010.

[13] A.Kush, Sunil Tanjea, "End to End Delay Analysis of Prominent On-demand Routing Protocols" IJCST, International Journal of Computer Sci ence and Technology, Vol 2 Issue 1 March 2011, I S S N : 2 2 2 9 - 4 3 3 3 (P r i n t) | I S S N : 0 9 7 6 - 8 4 9 1 (On l i n e) pp 42-46

[14] A.Kush, S.Taneja, Divya, "Encryption Scheme for Secure Routing in Ad Hoc Networks" in International Journal of Advancements in Technology http://ijict.org/ ISSN 0976-4860, **Vol 2, No 1 (January 2011)** pp22-29.