SECURE DATA TRANSFER FOR VARIOUS PATH SECURITY DESIGN FOR MOBILE AD HOC NETWORKS

M.Praveen [1],
Assistant Professor,
Department of CSE (AI&ML),
AVN Institute of Engineering and Technology

V. Sumadeepthi2
Assistant Professor,
Department of EEE,
G. Narayanamma Institute of Technology and Science

Mr.D.Prasad[3]
Assistant Professor,
Department of CSE,
St. Martin's Engineering College

ABSTRACT

Mobile ad hoc networks have self-organizing network architecture where a collection of mobile nodes with wireless network interfaces may form a temporary network without any established infrastructure or centralized administration. According to the IETF (Internet Engineering Task Force) definition a mobile ad hoc network is an autonomous system of mobile routers connected by wireless links. The mobile nodes can communicate without an infrastructure. Wireless networking is an emerging technology that will allow users to access information and services regardless of their geographic position. In contrast to infrastructure based networks, all nodes are mobile and can be connected dynamically in an arbitrary manner. Ad hoc networks proved their efficiency being used in different fields but they are highly vulnerable to security attacks and dealing with this is one of the main challenges of these networks today. Implementing security in such dynamically changing networks is a hard task. Sending confidential data on one path helps attackers to get the complete data easily. Whereas sending confidential data on multiple paths increases the security and confidentiality, because it is almost impossible to obtain all the divided message parts of an original message. In this study, we focus on improving the flow transmission confidentiality in ad hoc networks based on multipath routing. Indeed, we take advantage of the existence of multiple paths between nodes in an ad hoc network to increase the confidentiality &robustness of transmitted data. In our approach the original message is split into different parts that are encrypted and transmitted along different disjointed multiple paths between sender and receiver. In our solution, even if an attacker succeeds to obtain one or more transmitted message parts, the probability that the original message reconstruction is very difficult or almost impossible. Proposed technique is better compared to previous techniques.

Keywords –Mobile Ad Hoc Networks (MANET), Data Security Architecture (DSA), AES(Advanced Encryption Standard), Security.

I. INTRODUCTION

Mobile ad hoc networks have self-organizing network architecture where a collection of mobile nodes with wireless network interfaces may form a temporary network without any established infrastructure or centralized administration. According to the IETF (Internet Engineering Task Force) definition a mobile ad hoc network is an autonomous system of mobile routers connected by wireless links. The network's wireless topology may change rapidly and unpredictably. Nodes can be different wireless devices: PCs, mobile phones, handheld computers, printer's etc. Ad hoc network characteristics (dynamic topology, infrastructure less, variable capacity links, etc.) are origins of many issues like, Limited bandwidth, energy constraints, high cost and security are some encountered problems in these types of networks. Routing is an important aspect in ad hoc networks because of its special characteristics. Multiple disjointed paths can exist between nodes, thus multipath routing can be used to statistically enhance the confidentiality of exchanged messages

between the source and destination nodes.

Sending a confidential data on one path helps attackers to get the complete data easily. Whereas sending it in parts on different disjointed paths increase the confidentiality & robustness. In our solution, even if an attacker succeeds to obtain one or more transmitted message parts, the probability that the original message reconstruction is very difficult or almost impossible.

The data confidentiality is the protection of data from passive attacks such as eavesdropping while they are transmitted across the network. The wireless channel in a hostile environment is vulnerable to various forms of attacks, particularly the eavesdropping. A more severe problem in a MANET is that mobile nodes might be compromised themselves (e.g., nodes be captured in a battle field scenario) and subsequently be used to intercept secret information relayed by them.

One of the previous works is a SPREAD (Secure Protocol for Reliable data Delivery) scheme to statistically enhance the data confidentiality service in an ad hoc network. SPREAD is based on secret sharing and multi-path routing. Multi-path routing has been extensively studied in a wired network context for aggregating bandwidth, reducing blocking probability, and increasing the fault tolerance, etc. However, the shared wireless channel has a significant impact on the performance of multi-path routing.

In this the proposal of this work study the security performance of Data Security Architecture in multi-path with encrypted parted messages by simulation.

II. LITERATURE SURVEY

A few research works have been done to address the security issues in ad hoc networks. Security issues that have been addressed particularly for ad hoc networks include key management, secure routing protocols, handling node misbehavior, preventing traffic analysis, and so on. In this paper, we address the data confidentiality service in an ad hoc network. The data confidentiality is the protection of data from passive attacks such as eavesdropping while they are transmitted across the network. The wireless channel in a hostile environment is vulnerable to various forms of attacks, particularly the eavesdropping. A more severe problem in a MANET is that mobile nodes might be compromised themselves (e.g., nodes be captured in a battle field scenario) and subsequently be used to intercept secret information relayed by them. One of the previous works is a SPREAD (Secure Protocol for Reliable data Delivery) scheme to statistically enhance the data confidentiality service in an ad hoc network. SPREAD is based on secret sharing and multi-path routing. Multi-path routing has been extensively studied in a wired network context for aggregating bandwidth, reducing blocking probability, and increasing the fault tolerance, etc. However, the shared wireless channel has a significant impact on the performance of multi- path routing The aspect in which we are interested is security based multipath routing protocols. Multipath routing allows the establishment of multiple paths between a single source and single destination.

Security In Ad -Hoc Networks: -

In mobile ad hoc networks, security depends on several parameters (authentication, confidentiality, integrity, non-repudiation and availability). Without one of these parameters, security will not be complete. Without authentication, an attacker could masquerade a node, thus being able to have unauthorized access to the resources and to sensitive information. Confidentiality ensures that exchanged information will not be consulted by unauthorized nodes. Integrity means that information can only be modified by authorized users allowed to do it and by their own willing. Non-repudiation permits obtaining a proof that information are sent or received by someone. Thus, a sender or a receiver

cannot deny that he sent or received the concerned information. And finally, availability ensures that network services can survive despite any attack.

Ad hoc networks are exposed to many possible attacks. We can classify these attacks into two kinds: passive and active attacks. In passive attacks, attackers do not disrupt the operation of routing protocol but only attempt to discover valuable information by listening to the routing traffic. Defending against such attacks is difficult, because it is usually impossible to detect eavesdropping in a wireless environment. Furthermore, routing information can reveal relationships between nodes or disclose their IP addresses. If a route to a particular node is requested more often than to other nodes, the attacker will be able to expect that the node is important for the network, and disabling it could bring the entire network down.

Unlike passive attacks, active attacks are often detectable. An active attack can mainly be: Black hole attack, where a malicious node uses the routing protocol to advertise itself as having the shortest path to the node sending packets it wants to intercept. If the malicious reply reaches the requesting node before the reply from a correct node, a forged route is created. Thus the malicious node can do anything with the received packets. Another of active attacks is Routing tables overflow attacks. In this attacks, the attacker attempts to create routes to non-existent nodes. The goal is to create enough routes to prevent new routes from being created or to cause routing tables overflow. Sleep deprivation attacks is also an active attack where an attacker attempts to consume batteries by requesting routes, or by forwarding unnecessary packets. There are also location disclosure attacks which can reveal information about the node locations or the network structure and denial of service attacks (DoS), where an attacker can make the ad hoc network crashed or congested by different possible methods. Finally, we can cite impersonation attacks that we can avoid if node authentication is supported. Compromised nodes may be able to join the network while being undetectable or send false routing information

masqueraded as trusted node. There were the most important and dangerous possible attacks in ad hoc networks. To protect ad hoc networks against different kinds of attacks and to solve security problems, many approaches were proposed. We will see how can we classify them and what are their operating principles.

Secure Message Transmission:-

The Secure Message Transmission (SMT) scheme addresses data confidentiality, data integrity, and data availability in ad hoc network environment. The SMT scheme operates on an end-to end basis, assuming a Security Association (SA) between the source and destination nodes, thus, no link encryption is needed. This SA between end nodes is used to provide data integrity and origin authentication, but it could also be utilized to facilitate end-to end message encryption. The scheme works on top of the existing secure routing protocols, which cannot be themselves ensure data security. SMT uses multipath routing to statistically enhance the confidentiality and availability of exchanged messages between the source and destination nodes. Whereas SPREAD was primarily designed with the confidentiality of data transmission in mind, the designers of SMT focused primarily on the reliability of data transmission. In SMT each path is continually given a reliability rating that is based on the number of successful and unsuccessful transmissions on that path. SMT uses these ratings in conjunction with a multipath routing algorithm to determine and maintain a maximally secure path set and adjust its parameters to remain efficient and effective.

Secure Protocol for Reliable Data Delivery (SPREAD):-

The Security Protocol for Reliable Data Delivery (SPREAD) scheme addresses data confidentiality and data availability in a hostile ad hoc environment. The confidentiality and availability of messages exchanged between the source and destination nodes are statistically enhanced by the use of multipath routing. At the source, messages are split into multiple pieces that are sent out via multiple independent paths. The destination node then combines the received pieces to reconstruct the original message. The SPREAD scheme assumes link encryption between neighboring nodes, with a different key used for each link. Thus, to compromise confidentiality of a secret message, an adversary has to collect and decrypt all pieces of the message. Since each piece takes a different independent path, an attacker should be present in multiple locations at the same time to overhear or intercept all of the pieces.

Jigsaw Puzzle:-

The Jigsaw Puzzle scheme addresses data confidentiality and integrity in an ad hoc environment. Multipath routing is used to statistically enhance the confidentiality of exchanged messages between the source and destination nodes. The All- or-Nothing Transform is applied to a secret message to guarantee that no information can be obtained about the message unless all of its pieces are known. The message is then broken up into pieces by a jigsaw puzzle algorithm, which is based on operations with roots of polynomials. The pieces are transmitted across multiple node-disjointed paths. A Message Authentication Code (MAC) is transmitted with each piece to provide data integrity and origin authentication. Thus, it becomes impossible to compromise a secret message unless an adversary can eavesdrop close to the source or destination or simultaneously listen on all of the paths. In this method, the source and destination could share a secret prime number that could be used in the message division process.

Benefits of Multipath Routing:-

As mentioned before, multiple paths can provide load balancing, fault-tolerance, and higher aggregate bandwidth. Load balancing can be achieved by spreading the traffic along multiple routes. If multiple paths are used simultaneously to route data, the aggregate bandwidth of the paths may satisfy the bandwidth requirement of the application. Also, since there is more bandwidth available, a smaller end-to-end delay may be achieved. Due to issues at the link layer, using multiple paths in ad hoc networks to achieve higher bandwidth may not be as straightforward as in wired networks. Because nodes in the network communicate through the wireless medium, radio interference must be taken into account. Transmissions from a node along one path may interfere with transmissions from a node along another path, thereby limiting the achievable throughput.

III. IMPLEMENTATION

The idea behind our proposed system, First both sender and receiver has to exchange the message secret keys in secure fashion i.e. the secret keys are encrypted with session key. Then sender has to find the paths between source and destination then divide the initial message into ten message parts. Then sender has to enter secret key for each message part
and apply encryption algorithm after encryption select path for each part and send to destination. In receiver side the receiver has to enter secret keys for each message parts and apply the decryption algorithm to obtain original message.

Key Exchange:-

In this proposed system both sender and receiver should obtain the message secret keys in secure fashion. For this sender has to encrypt all message secret keys with session key using AES Encryption algorithm and send to receiver.

Multi-path Routing Topology (Paths Finding):-

The originality of the proposed approach is that it does not modify the existing lower layer protocols. The constraints applied in the security protocol are the sender `A' and the receiver `B' are authenticated, session key and message key is used for the encryption/decryption of message parts, a mechanism of discovering the paths of the network is available i.e. K-Shortest path algorithm.

Message Division:-

After path finding sender has to click on message division then system divides the initial message into ten message parts. While dividing initial message we considered MTU (Maximum transfer Unit) concept. Encryption of Messages in Multiple paths :-

For encryption sender has to enter secret keys for each message parts then apply AES algorithm for encryption. Parts identifiers are sent to allow the receiver to reconstitute the original message in the correct order. For fault tolerance problem, Diversity coding technique is used which is based on information redundancy.

Data Security Architecture (DSA):-

Design an application layer situated on top of the network (IP) layer that will manage the use of proposed two level data security solution to sent data securely Specific header, called DSA header will be added for useful information to ensure security. DSA layer is situated between two important layers. The first one is the IP layer that will provide our protocol with important information about routing, number of available routes, quality of routes, depending on the routing protocol used. The second layer is the transport layer (TCP/UDP) that is able to manage retransmission, if needed, especially when topology has changed.

IV. RESULT DISCUSSION

We used K-Shortest path algorithm for finding multiple paths between source and destination, the algorithm finds shortest path and remaining paths also. For Encryption and decryption we used AES (Advanced Encryption Standard) algorithm. We implemented simulation in Java using swing concept for GUI, Socket concept as networking tool. We knew the network topology for 4 nodes. Routes we considered are disjointed.. When executing the system the GUI Prompts Sender to enter destination node number and click on find paths then system returns the paths between source and destination. Then sender has to enter message or select the message file and click on message division then the system divides the original message into 10 message parts. Then sender has to enter secret key for each message parts after click on encrypt the system returns relevant cipher text, then sender has to select paths for each encrypted message parts. Then click on the send data. Based on path availability select paths for sending message parts. At the receiver side the receiver has to enter secret keys for each message pats then click on decrypt button then system returns the original message.

V. CONCLUSIONS

Proposed solution treats data confidentiality problem by exploiting a very important ad hoc network characteristic, which is the existence of multiple paths between nodes. Proposed system improves data security efficiently without being erroneous. It takes profit from existing ad hoc network characteristics and does not modify existing lower layer protocols. It is not complicated and can be implemented in different ad hoc devices. Proposed system is strongly based on multipath routing characteristics of ad hoc networks and uses a route selection based on security costs. If we used more paths for message transmission it provides more confidentiality and security.

FURTHER WORK

Nodes in an ad hoc network communicate through the wireless medium. If a shared channel is used, neighboring nodes must contend for the channel. When the channel is in use by a transmitting node, neighboring nodes

hear the transmission and are blocked from receiving from other sources. Furthermore, depending on the link layer protocol, neighboring nodes may have to defer transmission
until the channel is free. Even when multiple channels are used, the quality of neighboring transmissions may be degraded due to interference. Nodes within transmission range of each other are said to be in the same collision domain

REFERENCES

[1] A. Abdul-Rahman, S. Hailes, A Distributed Trust Model, in: Proc 97 New security paradigms, Langdale, Cumbria, United Kingdom, Sep 23–26 1997, pp. 48–60.

[2] N. Asokan, P. Ginzboorg, Key Agreement in ad hoc Networks, Computer Communications 23 (17)
(2000) 1627–1637.

[3] E. Ayanoglu, E. Chih-Lin, R.D. Gitlin, J.E. Mazo, Diversity coding for transparent self-healing and fault tolerant, Communication Networks: IEEE Transactions on Communications 41 (11) (1993)
1677–1686.

[4] A. Boukerche, K. El-Khatib, L. Korba, L. Xu, A secure distributed anonymous routing protocol for ad hoc wireless networks, Computer Communications Journal (2004). NRC 47393.

[5] A. Boukerche, K. El-Khatib, L. Xu, L. Korba, Secure ad hoc routing protocol, in: Fourth International IEEE Workshop on Wireless Local Networks. Tampa, Florida, É.-U. November 2004. NRC 47394.

[6] W. Diffie, M. Hellman, New directions in cryptography, IEEE Transactions on Information Theory IT-22 (6) (1976) 644–654.

[7] P. Gutmann, PKI: It's not dead, just resting, IEEE Computer (August) (2002) 41–49.

[8] http://www.cert.org/tech_tips/denial_of_service.html.

[9] Yih-Chun Hu, A. Perring, A survey of secure wireless ad hoc routing, IEEE Security and Privacy 2
(3) (2004). [10] M.M. Lehmus, Requirements of ad hoc network protocols, Technical report, Electrical Engineering, Helsinki University of Technology, May 2000.

[11] Qing Li, Yih-Chun Hu, Meiyuan Zhao, Adrian Perrig, Jesse Walker, Wade Trappe, SEAR: A secure efficient ad hoc on demand routing protocol for wireless networks, in: ACM Symposium on Information, Computer and Communication Security, ASIACCS 2008.

[12] Jing Liu, Fei Fu, Junmo Xiao, Yang Lu, Secure routing ad hoc networks, in: Software Engineering, Artificial Intelligence, Networking and Parallel/distributed Computing, 2007.

[13] L. Loukas, R. Poovendran, Cross-layer design for energy-efficient secure multicast communications in ad hoc networks, in: Proc of IEEE ICC 2004, Paris, France, May 2004.W. Lou, W. Liu, Y. Fang, SPREAD: Enhancing Data Confidentiality in mobile Ad hoc networks, in: Proc IEEE INFOCOM, Hong Kong, China, March 2004.

[14] J. Marshall, An analysis of SRP for mobile ad hoc networks, in: Proc of The 2002 International Multi-Conference in Computer Science, Las Vegas, USA, 2002.

[15] P. Papadimitratos, Z.J. Haas, Secure routing for mobile ad hoc networks, in: SCS Comm. Networks and Distributed Systems Modeling and Simulation, CNDS 2002, San Antonio, TX, Jan. 27–31, 2002.

[16] P. Papadimitratos, Z. Haas, Secure data communication in mobile ad hoc networks, IEEE Journal on Selected Areas in Communications 24 (2) (2006).

[17] M.R. Pearlman, Z.J. Haas, P. Sholander, S.S. Tabrizi, On the impact of alternate path routing for load balancing in mobile ad hoc networks, MobiHOC, 2000.

[18] A. Qayyum, Analysis and evaluation of channel access schemes and routing protocols for wireless networks, Ph.D. Dep Computer Science,

Paris XI. Paris Sud University, Nov 2000.
[19] M.O. Rabin, Efficient dispersal of information for security, load balancing and fault tolerance, Journal of the ACM 36 (2) (1989) 335–348.
[20] R.L. Rivest, All-or-Nothing Encryption and the package Transform, in: Fast Software Encryption Workshop, vol. 1267, Hafia, Israel, 1997, p. 210.
[21] A. Shamir, How to share a secret, Communications of the ACM 22 (11) (1979) 612–
613.
[22] B. Shrader, A proposed definition of ad hoc network, Royal Institute of Technology (KTH), Stockholm, Sweden, May 2002.
[23] F. Stajano, The Resurrecting Duckling—What Next? in: Proc 8th Security Protocols Workshop, in: Lecture Notes in Computer Science, vol. 2133
[24] Springer-Verlag, Berlin, 2001, pp. 204–