International Journal of Research Studies in Computer Science and Engineering (IJRSCSE)
Volume 1, Issue 1, May 2014, PP 52-56
www.arcjournals.org

Multi-Path Encrypted Data Security Architecture for Mobile Ad hoc Networks

Suresha k
Lecturer,Dept.of CS&E
DRR Govt Polytechnic
Davangere, Karnataka, India
skdrrgpt@gmail.com

S.B.Mallikarjuna
Associate Professor, Dept.of CS&E
Bapuji Institute of Engg. & Technology
Davangere, Karnataka, India
malliksb@yahoo.com

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 (MANETs), Data Security Architecture (DSA), AES (Advanced Encryption Standard), Security.*

1. 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, infrastructureless, 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.

2. 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.

3. 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

3.1. 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.

3.2. 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 neighbouring 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.

3.3. 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.

4. DATA SECURITY ARCHITECTURE FOR MOBILE AD HOC NETWORKS

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.

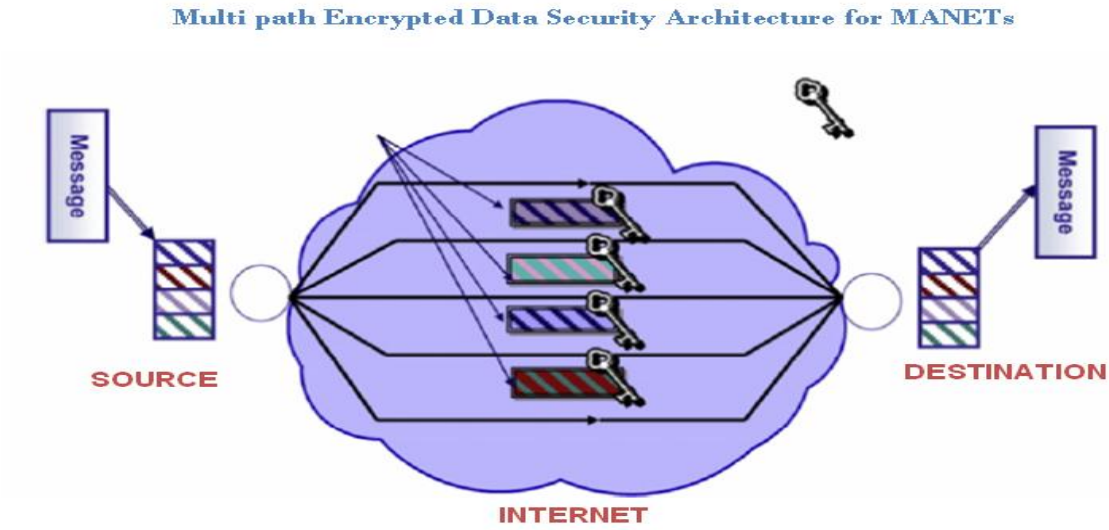

Figure 4.1. *System Architecture.*

Proposed System Modules

4.1. 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.

4.2. 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.

4.3. 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.

4.4. 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.

4.5. Path Selection

Sender has to select path randomly for each encrypted message parts

4.6. Send Data

After encryption and paths selection for each message parts sender has to send data to receiver.

4.7. Decryption

At the receiver side the receiver has to enter the secret keys for each received cipher text and apply AES Decryption algorithm to obtain original message.

5. 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.

6. IMPLEMENTATION & 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 Promts 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.

7. CONCLUSION

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.

REFERENCES

[1] Y.-C. Hu, A. Perrig and D. B. Johnson, "Ariadne : a secure on-demand routing protocol for ad hoc networks," MobiCom 2002, Sep 2002

[2] W. Lou, Y. Fang, "A survey of wireless security in mobile ad hoc networks: challenges and available solutions", book chapter in Ad Hoc Wireless Networking, Kluwer, May 2003

[3] P. Papadimitratos and Z. Haas, "Secure Routing for Mobile Ad Hoc Networks," Proc. SCS Comm. Networks and Distributed Systems Modeling and Simulation Conf. (CNDS '02), 2002.

[4] W. Lou, Y. Fang, "Securing data delivery in ad hoc networks", International Workshop on Cryptology and Network Security (CANS'03), Miami, FL, Sep 2003

[5] C.E. Perkins and E.M. Belding-Royer, "Ad-Hoc On-Demand Distance Vector Routing," Proc. Second Workshop Mobile Computing Systems and Applications (WMCSA '99), pp. 90-100, 1999.

[6] M.G. Zapata, "Secure Ad Hoc On-Demand Distance Vector Routing," Mobile Computing and Comm. Rev., vol. 6, no. 3, pp. 106-107, 2002.

[7] P. Papadimitratos and Z. Haas, "Securing Mobile Ad Hoc Networks,"Handbook of Ad Hoc Wireless Networks, M. Ilyas, ed., CRC Press, 2002.

[8] K. Sanzgiri, B. Dahill, B.N. Levine, C. Shields, and E.M. Belding-Royer, "A Secure Routing Protocol for Ad Hoc Networks," Proc. IEEE Int'l Conf. Network Protocols (ICNP '02), pp. 78-89, 2002

[9] Y.-C. Hu, D.B. Johnson, and A. Perrig, "SEAD: Secure Efficient Distance Vector Routing for Mobile Wireless Ad Hoc Networks," Ad Hoc Networks, vol. 1, no. 1, pp. 175-192, 2003.

[10] Y.-C. Hu, A. Perrig, and D.B. Johnson, "Packet Leashes: A Defense against Wormhole Attacks in Wireless Networks," Proc. IEEE INFOCOM, 2003.

[11] Y.-C. Hu and A. Perrig, "A Survey of Secure Wireless Ad Hoc Routing," IEEE Security and Privacy, vol. 2, no. 3, pp. 28-39, Mar. 2004.

[12] L. Buttya´n and I. Vajda, "Towards Provable Security for Ad Hoc Routing Protocols," Proc. ACM Workshop Ad Hoc and Sensor Networks (SASN '04), 2004.

[13] G. _ Acs, L. Buttya´n, and I. Vajda, "Provably Secure On-Demand Source Routing in Mobile Ad Hoc Networks," Technical Report 159, Int'l Assoc. for Cryptologic Research, 2004.

[14] G. _ Acs, L. Buttya´n, and I. Vajda, "Provable Security of On- Demand Distance Vector Routing in Wireless Ad Hoc Networks," Proc.European Workshop Security and Privacy in Ad Hoc and Sensor Networks (ESAS '05), pp. 113-127, 2005.

AUTHORS' BIOGRAPHY

S.B.Mallikarjuna received the Bachelor of Engineering (B.E) and Master of Technology (M.Tech) degrees in Computer Science and Engineering. Currently working as a Associate Professor in Department of Computer Science and Engineering at Bapuji Institute of Engineering and Technology, Davangere, Karnataka. He is currently pursuing Ph.D in Computer science and Engineering. Areas of Expertise Computer Networking, Formal Languages and Automata Theory, Operating Systems, Data Structures and Cloud Computing.

K.Suresha received the Bachelor of Engineering degree in Computer Science and Engineering from University B.D.T College of Engineering, Karnataka in the year 2003.He is currently pursuing M.Tech in Computer science and Engineering at Bapuji Institute of Engineering and Technology, Karnataka. Currently working as a Lecturer in the Department of Computer Science and Engineering at DRR Govt. Polytechnic, Davanagere, and Karnataka. Areas of interest include Network Security, Software Engineering, Programming with Java, Computer Organization.