Novel Technique of Multipath Routing Protocol in Ad hoc Network

Madhusudan G
Department of Computer Science & Engg.
SJCE,Mysore,India
Email: bms.madhu@gmail.com

D.S.Vinod
Department Information Science & Engg.
SJCE,Mysore,India
Email: dsvinod@daad-alumni.de

Abstract: *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. Recently, some solutions are proposed to provide authentication, confidentiality, availability, secure routing and intrusion detection in ad hoc networks. Implementing security in such dynamically changing networks is a hard task. Ad hoc network characteristics should be taken into consideration to be able to design efficient solutions. 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 to secure is split into different arrays that are encrypted are transmitted along different disjointed existing paths between sender and receiver. Even if an attacker succeeds to obtain one or more transmitted shares, the probability that the original message will be reconstituted is very low. We proposed novel technique in existing ad hoc multipath security solutions which is better compared to SDMP (Securing Data based Multipath Routing).The Proposed Method considers RSA Encryption technique both at sender and receiver sides.*

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. The 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 [10]. Ad hoc network characteristics are dynamic topology, infrastructure less, variable capacity links, etc. are origins of many issues. Limited bandwidth, energy constraints, high cost and security are some encountered problems in these types of networks. Denial of Service (DOS) attack in these networks aims to consume the scarce energy resource [8]. Using heavy solutions, like PKIs (Public Key Infrastructures) [2], is not efficient because of limited resources of ad hoc 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 whole of data to secure easily. Whereas sending it in parts on different disjointed paths

DOI : 10.5121/ijcnc.2012.4308

increases the confidentiality robustness because it is almost impossible to obtain all the parts of a message divided and sent on multiple paths existing between the source and the destination.

2. Security Aspects in Adhoc Networks

In mobile ad hoc networks, security depends on several parameters like authentication, confidentiality, integrity, non-repudiation and availability) [5]. Without authentication, an attacker could have unauthorized access to the resources information. Confidentiality ensures that exchanged information will not be consulted by unauthorized nodes. Integrity means that information can only be modified by nodes 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 namely 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. 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.

3. Different Models of Security

Recently, several researches interesting in ad hoc networks security aspects (like authentication, availability, secure routing, intrusion detection, etc) do exist. The Classification of existing approaches into different principal categories:

- Distributed Trust Models
- Key Management Models.
- Secure routing protocol Models.
- Intrusion Detection Systems
- Multipath protocols
- Proposed Novel Technique

Distributed Trust Model

The idea in is based on the concept of trust [1]. This protocol is used to exchange trust information.

Key Management

The basic concept in this approach [2] is the use of master/slave relations between devices. Master and slave share a common secret. This association can be only broken by the master. Duckling (slave) will recognize as mother (master) the first entity sending him a secret key on a protected channel. It is also called as key agreement based protocol.

Secure Routing Protocol

An important aspect of ad hoc network security is routing security [4][5].It provides correct information i.e., factual, up-to-date and authentic connectivity information regarding a pair of nodes that wish to communicate in a secure manner.

Intrusion Detection

It is one of the interesting aspects in wireless networks. It concerns detecting inappropriate, incorrect or anomalous activity in the network [26].

Multipath Routing

It allows the multiple paths between a single source and single destination node. It is typically proposed in order to increase the reliability of data transmission (i.e., fault tolerance)[3] or to provide load balancing [18]. Multipath routing has also been addressed in data networks which are intended to support connection oriented service with QOS like in ATM.

Secure Message Transmission

The Secure Message Transmission (SMT) 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.

Security Protocol for Reliable Data Delivery

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.

Securing data based multipath routing in ad hoc networks (SDMP) The idea behind this protocol is to divide the initial message into parts then to encrypt and combine these parts by pairs. Then exploit the characteristic of existence of multiple paths between nodes in an ad hoc network to increase the robustness of confidentiality. This is achieved by sending encrypted combinations on the different existing paths between the sender and the receiver. In this method even if an attacker succeeds to have one part or more of transmitted parts, the probability that the original message can be reconstructed is low. We start by presenting our method principle. At first, we present the principle of SDMP protocol in a simplified scheme in figure 1, and then we explain in detail how it works. The originality of our approach is that it does not modify the existing lower layer protocols. Some assumptions should be taken into consideration:

- The sender `A' and the receiver `B' are authenticated,
- Wired Equivalent Piracy (WEP) or Temporary Key Integrated Protocol (TKIP) is used for the encryption/decryption of frames at Medium Access Control (MAC) layer and the authentication of the terminals,
- A mechanism of discovering the topology of the network is available,
- The protocol uses a routing protocol supporting multipath routing.

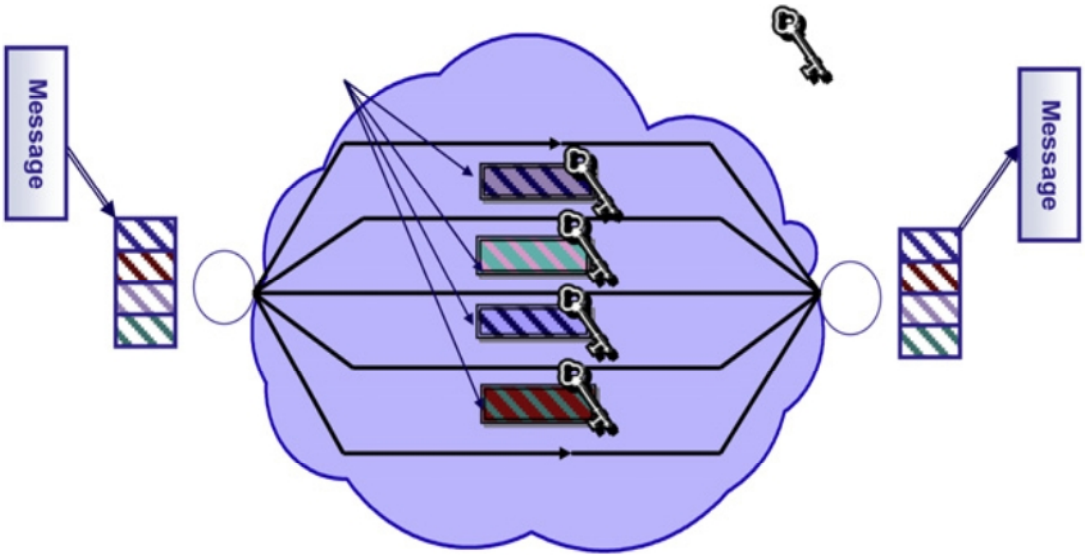

Fig. 1. Principle of SDMP.

In this protocol, the first important information need is the network topology. The protocol will use n routes (the message will be divided into n - 1 shares): one path is used for signaling (we called signaling channel), a second one is used to transmit in plain text a key share (randomly chosen) used to initiate the de combination process and the others (n - 2 paths) are used to transmit the different shares of the original message. For these reasons, we should have at least 3 links.

The original message m is divided into (n - 1) shares; each of them has a unique identifier. The protocol generates, a random number x($1< x \leq (n- 1)$, x integer) to be sent on the signaling channel, then code shares in pairs using an XOR operation related to x. The x share will be transmitted in plain text. Every combination is sent over one of the remaining (n - 1) channels.
The x part is sent in plain text on one of the n paths. It will be the start point for receiver to find other parts as explained in figure 2.

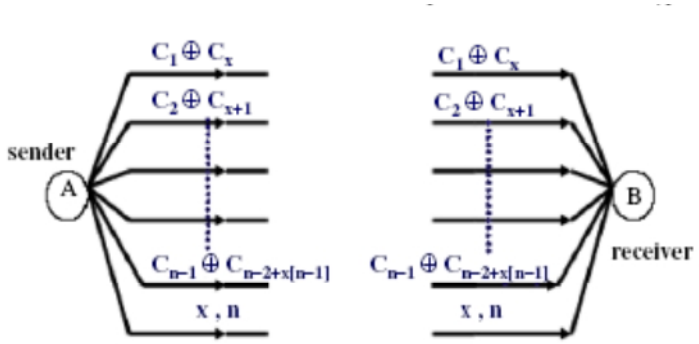

Fig. 2. SDMP combination algorithm.

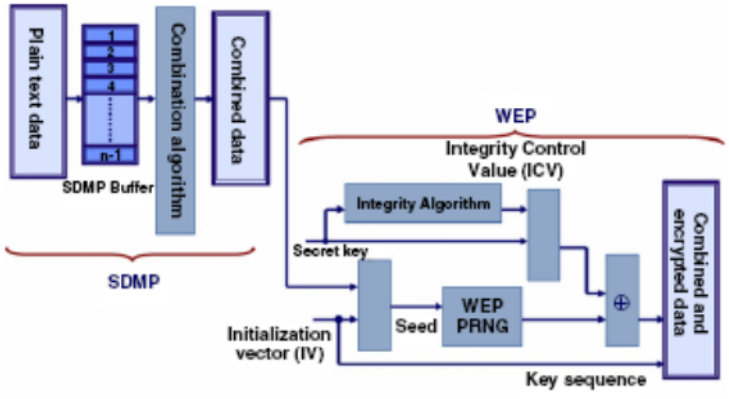

Fig. 3. Combination–encryption process.

Results of the combination of every pair of the message parts on every data channel are sent encrypted by WEP to reinforce confidentiality. It can note that we have chosen WEP for experiments. This gives a double shielding to the data confidentiality. Combination of SDMP with WEP can be performed as it is represented in figure 3. Parts' identifiers are sent to allow the receiver to reconstitute the original message in the correct order. For fault tolerance problem, one can also use Diversity Coding technique which is based on information redundancy.

Architecture of Secured Data based Multi Path Protocol

As illustrated in Fig. 4, we add a layer situated on top of the network (IP) layer that will manage the use of the solution to secure sent data. Specific header, called SDMP header will be added for useful information to ensure security. SDMP 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 after the data transmission had started. The

Secured Data based Multi Path Protocol (SDMP) introduces a set of features that can be incorporated with low overhead without modifying lower layer protocols. Both sender and receiver should implement SDMP layer to be able to use this protocol.

Before sending data between sender (A) and destination (B), the topology is provided in order to calculate the different routes n between A and B. If n<3, a message error is generated, otherwise the n routes that will be used to transmit data securely will be chosen from the n existing routes according to a cost function.

Paths selection in SDMP In an ad hoc network the topology changes frequently, which makes wireless links instable. Sometimes packets might be dropped due to the bad wireless channel conditions, the collision at MAC layer transmission, or because of out of date routing information. When packet loss does occur, non-redundant share allocation will disable the reconstruction of the message at the intended destination. To deal with this problem, it is necessary to introduce some redundancy (if there is enough paths) in SDMP protocol to improve the reliability, (i.e. the destination would have better chance to receive enough shares for reconstructing the initial message). We propose that the decision of using or not redundancy will be taken according to the average mobility of the network's nodes and to the existing path number. SDMP is based on multipath routing in ad hoc networks.

Fig. 4. Protocol stack.

4.0 Proposed Method

Further to enhancing the security provided by the SDMP routing protocol an enhancement to the same can be provided. This enhancement is based on the concept of partition. **The partition** of a positive integer *n*, also called an **integer partition**, is a way of writing *n* as a sum of positive integers. Two sums that differ only in the order of their summands are considered to be the same partition. For example, 4 can be partitioned in distinct ways:

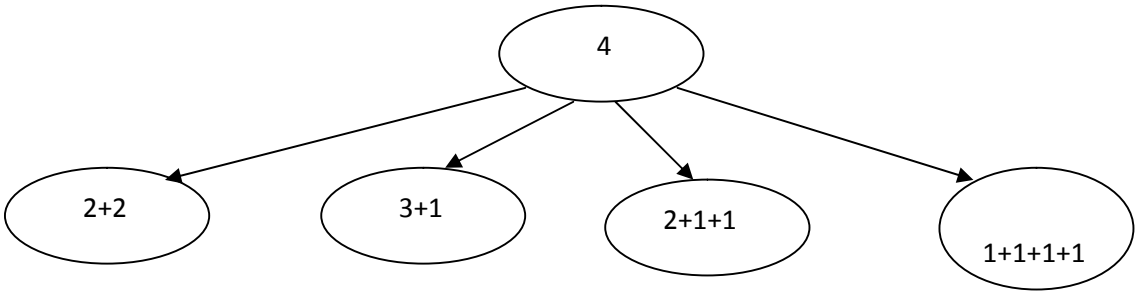

Fig.5, Tree Structure of Partition

The concept of partition can be used in enhancement of the proposed implementation of the SDMP routing protocol in the following way: The proposed implementation of the SDMP routing protocol requires that an array, say ***a*** needs to be sent across from the sender of the message to the recipient. This array ***aids*** in the de-combination process at the receiver by providing the part numbers for subsequent de-combination. Interception of this array in its original form can hinder the proposed security to an extent. Hence further processing can be done on this array before sending to enhance the effectiveness. This can be done through the concept of partition. Here, a partition constant p_k can be used which will be known only to the sender and the receiver. The constant p_k can be used to translate the array a as follows:
At the sender, the array a can be translated as:

- q[i] = pk -a[i], for all i from 1 to (number of message parts)
  Then, the SDMP implementation sends q rather than a.
- At the receiver , the array a can be obtained back as:
  a[i] = pk - q[i], for all i from 1 to (number of message parts)

This ensures further security enhancement of the SDMP routing protocol implementation.

Pseudo Code of the Algorithm

Input: At the Sender A Read and display the message to be transmitted. Apply RSA algorithm for the encryption.

N: Total number of Paths.

A&B: Sender and Receiver.

D: Decomposition.

n:The input Message.

x : Part of the Message.

Input: int paths ( ) //{Total Paths }

Return the number of total paths between A and B, by looking at whether the network topology has changed

Function int select (int N, String msg) // {Select Paths}

paths = msg.length ( ) /8 //An arbitrary logic to select paths used for transmission out of N

Based on the value of paths, select the paths, such that, it is greater than or equal to 3 and lesser than or equal to N//

Function String [ ] divide (String msg, int n) // {Divide Message}

Divide the message equally into the number of paths selected. The last path will contain the remaining message which will be greater than or equal to msg piece length.

Function int selectpp (int n) //{ Plain Part}

Select and return a random message part as the plain part to initiate the combination process

Function {Combine Parts}

d[] = int[100] //Gives the subscript of the message part to be used for the corresponding de combination process

Function {XOR Encrypt}

String encrypt (String part1,String part2) perform XOR operation on the two parts.

Function {De combine}

String[] de combination(String combination[],String plainpart, int arr[], int n, int x)

Function { XOR decrypt }

String decrypt(String s1,String s2) Perform XOR operation on the two parts.

Function { Rsa Algorithm} int mult(int x,int y,int n)

k <- 1, for j from 1 to y

k <- (k*x)%n

return (int)k

Function String encrypt(String s)

n <- 253, e <- 13, Convert string to integer array, pt[]

for i from 0 to s.length()-1

ct[i] <- mult(pt[i],e,n)

Convert ct[] to string and return

Function String decrypt(String s)

n <- 253, d <- 17, Convert string to integer array ct[]

for i from 0 tp s.length()-1

pt[i] <- mult(ct[i],d,n), Convert pt[] to string and return.

Output: At the receiver B, Apply RSA decryption Algorithm to decrypt the received message.

Table 1. Protocol Comparisons

Protocol	SMT	SPREAD	SMDP	NOVEL
Confidentiality	YES	YES	YES	YES
Integrity	YES	NO	YES	YES
Availability	YES	YES	YES	YES
Used Encryption	End to END	Link	Link	RSA

Table 1 describes the different protocol comparisons considering the security issues like Confidentiality, Integrity, Availability and used Encryption. The different Protocol Considered are SMT, SPREAD, SMDP and NOVEL Method. The Novel Technique considers RSA Encryption technique both at the sender and receiver sides.

5.0 CONCLUSION

In this paper, a new solution was analyzed that treats data confidentiality problem by exploiting a very important ad hoc network characteristic, which is the existence of multiple paths between nodes. The solution improves data security efficiently without being erroneous. It takes profit from existing ad hoc network characteristics and does not modify existing lower layer protocols. This protocol is strongly based on multipath routing characteristics of ad hoc networks and uses a route selection based on security multipath. The more number of used paths is important, the more confidentiality is enforced. Using multiple paths allows us taking profit from using some redundancy that decreases probability of dropping messages. SDMP protocol can be combined with other solutions which consider other security aspects than confidentiality to improve significantly the efficiency of security systems in ad hoc networks.

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.

[14] W. Lou, W. Liu, Y. Fang, SPREAD: Enhancing Data Confidentiality in mobile Ad hoc networks, in: Proc IEEE INFOCOM, Hong Kong, China, March 2004.

[15] 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.

[16] 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.

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

[18] 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.

[19] 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.

[20] M.O. Rabin, Efficient dispersal of information for security, load balancing and fault tolerance, Journal of the ACM 36 (2) (1989) 335_348.

[21] R.L. Rivest, All-or-Nothing Encryption and the package Transform, in: Fast

Software Encryption Workshop, vol. 1267, Hafia, Israel, 1997, p. 210.

[22] A. Shamir, How to share a secret, Communications of the ACM 22 (11) (1979) 612_613.

[23] B. Shrader, A proposed definition of ad hoc network, Royal Institute of Technology (KTH), Stockholm, Sweden, May 2002.

[24] F. Stajano, The Resurrecting Duckling_What Next? in: Proc 8th Security Protocols Workshop, in: Lecture Notes in Computer Science, vol. 2133, Springer-Verlag, Berlin, 2001, pp. 204_214.

[25] R.A. Vasudevan, S. Sanyal, A novel multipath approach to security in mobile ad hoc networks, in: International Conference Computers and Devices for Communication, Kolkata, India, Jan 2004.

[26] Y. Zhang, W. Lee, Y. Huang, Intrusion detection techniques for mobile wireless networks, ACM MONET Journal (2002).