EFFICIENT SECURITY APPROACHES IN MOBILE AD-HOC NETWORKS: A SURVEY

Prashant Sangulagi[1], Naveen A S[2]

[1]*Department of Electronics and Communication, BKIT, Bhalki, India: 585328*
[2]*Department of Electronics and Communication, BKIT, Bhalki India: 585328*

Abstract

Mobile Ad-Hoc Networks (MANET's) are the one of the popular and ongoing research where nodes exchange their information without forming predefined network (infrastructure less based network), so maintaining data secrecy and data confidentiality is an important and challenging task. In order to secure data, one has to deploy security technique either at the transmitter side or at the medium side (Channel) so that attacker or third party should not access the information. In this paper we are surveying some of the efficient security techniques available in MANETs considering both possible ways i.e. security either can be employed at the transmitter side or between links. Survey says that SMT technique holds good in all aspects where SPREAD and SDMP provides security but increases system overhead.

Keywords: *MANET, Data Security, SMT, SPREAD, SDMP.*

---***---

1. INTRODUCTION

Mobile Ad-hoc networking (MANET) is a self-configuring network architecture in which a group of mobile nodes, they may built a temporary network without the help of any centralized ministry or established infrastructure. The nodes are free to move independently in any direction.

Security is extremely important problem in a mobile ad hoc network (MANET). In comparison with an wired or infrastructure network, a mobile ad hoc network(MANET) poses many new challenges in security. For example, wireless channel is more uncovered to passive attacks (eavesdropping), or active attacks (signal interference and jamming); the co-operative MANET protocols are more exposed to denial of service attacks; the deficiency of infrastructure and limited resources restrict the use of some conventional security solutions; and the un-predictable ad hoc mobility makes it more difficult to detect harmful behavior[1].

Because of these many new challenges, most of security solutions that are applicable in a wired network become in applicable in a MANET. Much effort has been made to develop suitable security solutions that suites to a MANET environment. Among them, key management, may be the most critical and fundamental security problem in a MANET, has attracted much focus [2, 3, 4]. Many numbers of secure routing protocols have also been proposed in order to protect the correctness of different types of ad hoc routing protocols, both table driven and distance vector routing types [5].

The method discussed in this survey paper addresses the data confidentiality service in MANET. Data confidentiality means protection of the transmitted data from passive attacks (i.e. eavesdropping). It requires data integrity, data confidentiality and data availability for sensitive information, such important military information transmitted across war field (an ad hoc network). Leakage of such information to the outers (i.e. enemies) could lose its value. The wireless channel in an unfriendly environment is uncovered particularly to passive attacks (i.e. eavesdropping). Message transmitted through the open area can be eavesdropped from anywhere without having any physical contact to the network components.

Confidentiality in MANET is achieved by cryptography. However, the limited resources, such as processing capability, limited battery power and small size, confine the use of very good encryption schemes in a MANET. Sometime computationally efficient encryption schemes are not secure enough. For example, the WEP (Wired Equivalent Privacy) protocol defined in IEEE 802.11 uses RC4 algorithm, and computationally efficient. But, it has been discovered that it can be decrypted through traffic analysis. Usually mobile nodes resides in open and unfriendly environment, is the more secure problem in MANET. Formerly nodes themselves might be compromised in the war-field scenario, nodes might be captured. In this case, all the security information stored in the nodes would be compromised, including keys. In this case any encryption scheme would not help, no matter how secure enough it is. The secured communication in MANET consists of three phases. Firstly, how to dividing the secret message into number of piece?. Secondly, how finding the multiple paths in MANET?. Thirdly, how piece of message given to selected path.

2. SECURE DATA TRANSMISSION USING MULTIPATH ROUTING

The schemes SPREAD [6], SMT [7], SDMP [8], are analyzed, compared and made survey that intention to improve data security and confidentiality, availability and integrity in unfriendly and timely changing MANET environments. These above schemes use many paths between end nodes to drastically improve data confidentiality, data availability and data integrity. Above three schemes address data confidentiality, data availability and data integrity. It does not mean that data confidentiality, data availability and data integrity all supported by all above schemes.

Apart from the above three schemes the basic one is Secure Single Path (SSP) is an end-to-end secure data transmitting protocol that utilizes a single route. Unlike above three, SSP does not include any multi-path transmission overhead. And it does not require any multipath finding routing protocol either. Thus, SSP imposes less routing overhead than all above schemes. Overall, SSP and compare it to above three as an alternative, lower cost, more flexible protocol to secure the data transmitting cycle. The reason for not using of SSP is that, it does not provide data confidentiality, data integrity and data availability in unfriendly environment.

2.1 Secure Protocol for Reliable Data Delivery (SPREAD)

The Secure protocol for reliable data delivery (SPREAD) scheme addresses both data confidentiality and data availability in an unfriendly MANET environment [6]. The confidentiality and availability is statistically improved for the messages which transmitted between the source and destination nodes by the use of multipath routing. At the source, messages are dividing into multiple pieces that are sent out by means of many independent node disjoint paths. The destination node receives the message pieces and combines them to reconstruct the original message. The SPREAD uses link encryption between adjacent nodes, with different key for each link. To compromise the secret message, enemy must fulfill at least two things. First, the enemy has to collect all the pieces of secret message by either compromising or eavesdropping nodes. Second, as we uses the link-encryption between adjacent nodes each link with different keys. By this, even if enemy collects all the pieces of secret message, he has to decrypt them.

The SPREAD scheme uses the *(K, N)* threshold secret sharing algorithm to divide the secret message into multiple pieces. Suppose we have secret message and we divided it into *N* pieces, called shares. Each of *N* participants of secret message holds one share of the secret respectively. At least *K* participants must require for reconstructing the secret message, any less than this will not acquire anything about the system secret, while with *(K, N)* threshold secret sharing scheme, any *K* out of *N* participants can reconstruct the secret message. By the use of*(K, N)* threshold secret sharing algorithm, the secret message can be divided into *N* message shares in order to compromise the message; the enemy must compromise at least *K* shares of the message. With less than *K* message shares, the enemy could learn nothing about the secret message and he has no better option to learn about the message who knows nothing about it. SPREAD uses *(K, N)* Threshold Secret Sharing with multipath routing to carry out successful data confidentiality, wherever an opponent must compromise all of the utilized paths to compromise secret message. In order to compromise any given paths, an opponent must compromise at least one node from every path. Formally, let P_s denote the probability that a given path s is compromised and let q_r denote the probability that a given node r on path s is compromised. It follows that $P_s = 1 - (1 - q_1)(1 - q_2)\ldots..(1 - q_n)$, where nodes 1,2,…,n to consists of path s, Assume that a total of M independent paths are utilized to transfer an secret message. Thus, the probability Pmsg that a secret message is compromised under best data confidentiality is given by Pmsg = $\prod_{S=1}^{M} p$s.

Best confidentiality of data is negligibly achieved when *K=N*, and between 1 and *K – 1* shares are allocated to each utilized multipath. Nevertheless, to enhance data availability there introducing redundancy should be compulsory by choosing *K<N*. This choice of *K* given confidentiality that the original message can be reconstructed in the presence of topological changes, node failure, or active attacks as long as no more than *N – K* shares are lost. It can be shown that allocating between *N –K + 1* and *K – 1* secret message piece to each path provides best data confidentiality when redundancy is introduced. Thus, even if a small number of secret message shares are compromised, the confidentiality of the original message remains uncorrupted.

2.1.1 Maximal Node Disjoint Path Finding Algorithm(MNDPFA)

The algorithm proposed in SPREAD scheme is modified from the node disjoint shortest pair algorithm [9]. The modified Dijkastra algorithm is used find maximal route, which modifies the standard Dijkastra algorithm. This modified Dijkastra allows changing back to tentative (i.e. a trail) label from permanent when a lesser cost to that node is found.
Consider a MANET as shown in fig. then, how to find multipath by using modified Dijkastra algorithm?
Step1: Encounter the first most secure path by modified Dijkastra algorithm from source S to destination D as S – N1 – N2 – D, then replace all links involved in that path by an arrow which are towards the destination S - > N1 - > N2 - > D.
Step 2: Split each node involved in that path as a two sub nodes except source and destination and made arrow directed towards source (i.e. this path is already selected find the other

than this). Cost between two sub nodes should be ‘0’ and others should be ‘-1’.

Step 3: The links which are connected to these should replace by arrow in such a way that one is approaching and one is leaving the nodes.

Step 4: Replace all the links of the nodes which are connected to the separated sub nodes (i.e. N1 and N2) by arrow that should be directed towards destination i.e. here N3, N4, N5 are connected to N1 and N2 is replace the links of N3, N4, N5 by arrow.

Step 5: Now forms recently made path from source to destination that should be in such a way that the cycle should not be formed. By this another path will be formed between source and destination via N5 and N6 as routers.

Step 6: Now indicate this new path along with the path find in first step 1.

Step 7: continue the same procedure from step 2 i.e. now we got two paths, we have to spilt all the nodes involved in these 2 paths into sub nodes and continue the same to get more possible path (i.e. continue till no more paths available).

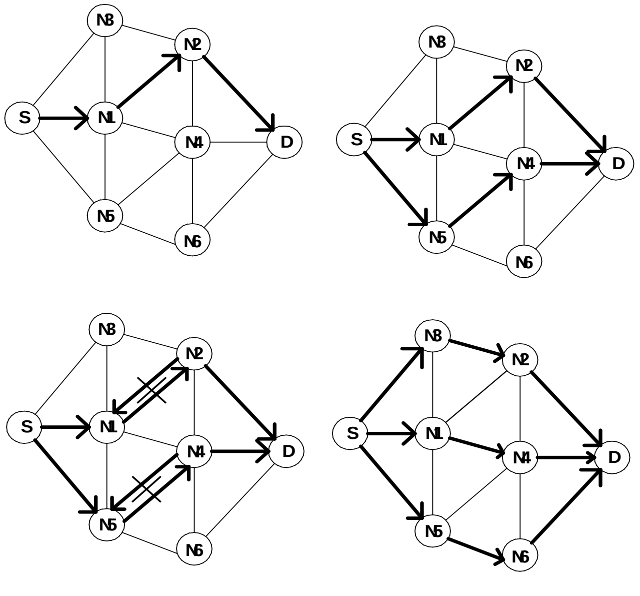

Fig 1: Maximal node disjoint path algorithm

2.2 Secure Message Transmission (SMT)

The Secure message transmission (SMT) scheme addresses data integrity, confidentiality and availability in a highly unfavorable and mobile MANET environment [7]. The SMT scheme works on an end-to-end basis, believing that the Security Association (SA) between only the source and the destination nodes, so no link encryption (i.e. as like of SPREAD) is not needed. This Security Association (SA) between source and destination nodes is used to provide data integrity and origin authentication, but it could also provide easier end-to-end message encryption.

As same as SPREAD scheme, SMT uses multipath routing to drastically increase the data availability and data confidentiality of shared message between the source and destination nodes. SPREAD was basically designed with the confidentiality of data transmission in mind, SMT focused basically on the reliability of data transmission. SMT provides a clear end-to-end secure and strong feedback mechanism that allows for fast reconfiguration of set of paths in case of node compromising or node failure. Depends upon the number of successful and unsuccessful transmissions each path is continually assigned with reliability rating. An SMT uses these ratings along with a multipath routing algorithm for maintain and determine a maximally secure set of paths and adjust its parameter to remain effective and efficient (as SMT tries to select shortest- hop paths, so data confidentiality is also considered).

This scheme uses Information Dispersal Algorithm (IDA) [10] that divides the message to multiple pieces along with finite redundancy. Every single piece of message is transmitted on a different node-disjoint path. With each piece a Message Authentication Code (MAC) is transmitted to provide data integrity and origin authentication. The information redundancy factor is the ratio of N/M where any M message pieces are necessary to reconstruct the original message out of N piece of transmitted message. It is important that, unlike threshold secret sharing algorithm case, it is not guaranteed that less than M pieces will not resemble any information about the transmitted message. Guaranteed reconstruction of the transmitted message at the destination, even if some of the pieces are lost in the network are provided by the data redundancy paired with multipath routing. By this reconstruction of lost packet are often excluded, which strongly allows SMT to support real time traffic with Quality of Service requirements.

The simulation results for SMT show that this scheme can successfully manage with a large number of opponents in the network. In fact, more than twice the number of packets that can be successfully delivered in SMT by a protocol employs secure route discovery but no secure data forwarding. In addition, a lower end-to-end delay is achieved in SMT than the schemes employing unipath routing. Lower end-to-end delay is enabled by multipath routing. This difference is increased as the number of enemy in the network increase. In the presence of opponent, routing overhead is lower than with unipath (e.g. SSP) schemes, because the use of multiple paths allows for less common route discoveries in the case of path failures. However, SPREAD and SMT imposes larger network band width overhead than that of unipath schemes.

An example for transmission of message in SMT is shown in Fig 2. The sender divides the encoded message into four packets of messages, so that any three out of the four packets are enough for the successful reconstruction of original message. The four packets are transmitted over four disjoint paths and two out of them arrive successfully at the receiver. The remaining two packets are compromised by malicious nodes present on the corresponding paths; for example, one packet (dashed arrow) is modified, and one is dropped.

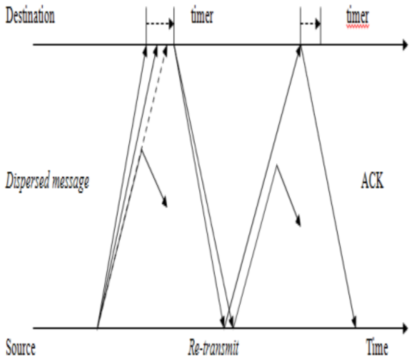

Fig 2: Example for transmission of message using SMT

The receiver decoction the information from the first incoming validated packet and waits for the subsequent packets, with a reception timer on. When the last packet among the divided message received, the cryptographic integrity checks if it is unauthorized then the packet is rejected. At the expiration of the timer which is set at the receiver, the receiver sends an acknowledgement to sender reporting the two successfully received packets and feedbacks the acknowledgment across the two operational paths belongs to that particular packet. By ignoring the duplicates, the sender will cryptographically validate only one acknowledgment. The two failed paths are neglected and the missing packets are retransmitted along the two new different paths; again one out of two packets is lost, for example, because of intermitted malicious response, or node is compromised. Before the timer expiration, the receiver will acknowledge the successful reception, since a sufficient number of packets (3 out of 4 packets) have been received. It is important that after transmission of the first packet, the sender sets a retransmission timer, so all the acknowledgment can be detected.

2.2.1 Information Dispersal Algorithm

Information Dispersal Algorithm was proposed by Rabin to make easier data redundancy [10]. With this ID algorithm, a file M is divides into n pieces and out of n any m pieces can be sufficient to reconstruct M file. Here n and m are positive integers, with m always less than or equal to n ($m \leq n$). This algorithm was proposed to improve the trustworthy of communication networks and disk storage system in the presence of failures. For example file M may be divided into several pieces and each piece is routed on different network paths, from the sender to receiver, such that the failure of one or more disks will not results in data loss. The amount of redundancy introduced should be proportional to the possibility of failure.

The proposed ID algorithm is based on simple matrix operations. Suppose that the file M consists of L bytes: $M = b_1, b_2, \ldots, b_L$, where $0 \leq b_j \leq 255$. A prime number $p > 255$ is chosen; for example $p = 257$. Next, n random vectors a_j of length m are chosen and structured as rows of on $n * m$ matrix A, such that any m different vectors are linearly independent: $a_j = (a_{j1}, a_{j2}, \ldots, a_{jm})$. The file M is divided into byte sequences of length m: $M = (b_1, \ldots, b_m), (b_{m+1}, \ldots, b_{2m}), \ldots = P_1, P_2, \ldots$ The vectors P_j are multiplied by the vectors $a_j$to form the set of divided M file pieces: $F_1, F_2, \ldots, F_n$. All arithmetic operations are takes place in the limited field Z_p, that is, modulo p. To reconstruct the original message file M, only m pieces are required: $M_1, M_2 \ldots M_m$. Every m piece of message is multiplied by A^{-1}, the inverse of matrix A containing only rows corresponding to the indices of the available message pieces.

This ID algorithm has fair time complexity since the necessary matrix operations can be implemented in a simple and effective manner, with complexity of at most $O(n^3)$. The space overhead required ny the algorithm for data redundancy is most favorable since each of the n pieces is of size $|M|/m$ here $|M|$ denotes the size of M. In other words, if $|M|$ isφ bytes, then the total size of the produced pieces will be $n * (\varphi/m) = (n/m) * \varphi$ bytes. Thus, the space overhead needed for data redundancy is exactly proportional to the redundancy factor n/m, which is skillfully the best case possible. The signaling overhead imposed by information dispersal algorithm is quite manageable. Knowledge of the identifying indices of the pieces is required for reconstruction of M; these can be easily bundled with the message pieces. Even though matrix A is reused many times to reduce overhead, knowledge of the random A is required.

2.3 Secure Data Based Multipath Routing (SDMP)

The Secure Data Based Multipath Routing (SDMP) scheme mainly gives the data confidentiality in a MANET environment [8]. The SDMP scheme assumes Wired Equivalent Privacy (WEP) link encryption between adjacent nodes, which provides link layer authentication and confidentiality. The confidentiality of transferred message pieces between the source and destination nodes is statistically increased with the help of multipath routing. SDMP is provided with an existing multipath routing process, making no assumptions about the node-disjointness of the supplied set-of path. There must be at least three paths to be present between source and destination in SDMP because one path is dedicated for signaling.

The original message is divided into pieces and provided with a unique identifier in the SDMP scheme. Message pieces are XOR-ed, and each pair is transmitted along a different path. This approach for message division is essentially a non-redundant version of Diversity Coding [11]**.** Even redundancy could be easily added to provide data availability. Information concerning the pair combinations is sent on the signaling path to allow message reconstruction at the destination. The data is assigned to each path according to the path cost function in order to minimize the time spent at the receiver side to reconstruct the original message. Unless the enemy can give access to the all transmitted piece of message, the possibility of message reconstruction is low. This means, to compromise the confidentiality of the original secret message, the attacker must get within eavesdropping of the destination or source or simultaneously listen on all the paths used and decrypt the WEP encryption of transmitted piece of message. However, it requires only few pieces of transmitted message at the destination side are enough to reconstruct the original message, especially since one piece of the original message is always sent in its original form on one of the selected paths.

SDMP simulation results shows that the time to send a large message notably increases as number secure paths used are more. However, using more secure paths increases the confidentiality. Thus, there is a trade-off between the security and delay of a given message. It should be notable that the use of a devoted signaling path simplifies the protocol, but also leads to notable waste of network resources. That is, a notable amount of overhead is required to discover and maintain an extra path that is used to periodically send small amounts of protocol control information; furthermore, this signaling path creates a single point of failure in SDMP. If an opponent can jam or compromise this path, the entire scheme will stop useful operation until another signaling path can be established.

3 COMPARISONS OF SPREAD, SMT, AND SDMP

Here comparison is made among SPREAD, SMT and SDMP based on some parameters, like confidentiality addresses, integrity addresses, availability addresses, message division algorithm, encryption type, layers of operation and optimization of path. Based on the factors suitable scheme will be selected.

Table 1: Comparisons of SPREAD, SMT, and SDMP

Scheme	**SPREAD [6]**	**SMT [7]**	**SDMP [8]**
Confidentiality Addressed	Yes	Yes	Yes
Integrity Addressed	No	Yes	no
Availability Addressed	Yes	Yes	No
Message Division Algorithm	Threshold Secret Sharing [12]	Informatio n Dispersal [10]	Diversity Coding [11]
Encryption Type	Link	End-to-end	Link
Layer of Operation	at Network	at Network	above Transport
Path-set Optimized	Yes	Yes	No

4. CONCLUSIONS

Data security and data confidentiality are important issues in MANETs especially when the data is highly confidential one. In this paper we have gone through the some of the popular security techniques in MANETs. Survey shows that SMT provides end to end security and path set is optimized as well as there is no such affection the overall system performance. SPEARD provides Security at link side and compare to SMT it provides more confidentiality but system overhead is more here. SDMP also provides security at link side and in this also system overhead problem arises as number of links increase when the message is large. Hence we can conclude the SMT Technique hold good in all the aspects then compare to SPREAD and SDMP.

REFERENCES

[1]. W. Lou, Y. Fang, “A survey on wireless security in mobile ad hoc networks: challenges and available solutions”, book chapter in Ad Hoc Wireless Networking, to be published by Kluwer in May 2003

[2]. J-P. Hubaux, L. Buttyan and S. Capkun, “The quest for security in mobile ad hoc networks”, MobiHOC'01, 2001

[3]. L. Zhou and Z. J. Haas, “Securing ad hoc networks”,' IEEE Network Magazine, vol. 13, no. 6, November/December 1999

[4]. J. Kong, P. Zerfos, H. Luo, S. Lu and L. Zhang, “Providing robust and ubiquitous security support for manet”, Proceedings of the 9th IEEE International Conference on Network Protocols(ICNP), 2001.

[5]. Y.-C. Hu, D. B. Johnson and A. Perrig, “SEAD: secure efficient distance vector routing for mobile wireless ad hoc networks”, WMCSA'02, June 2002

[6]. W. Lou, W. Liu, and Y. Fang. “SPREAD: Enhancing Data Confidentiality in Mobile Ad Hoc Networks”. Hong Kong, China, March 2004. IEEE Conference on Computer Communications (INFOCOM’04).

[7]. P. Papadimitratos and Z. J. Haas. “Secure Data Transmission in Mobile Ad Hoc Networks” Atlanta, Georgia, USA, September 2003. International Conference on Web Information Systems Engineering (WISE’03)

[8]. S. Bouam and J. B. Othman. “Data Security in Ad Hoc Networks Using Multi- Path Routing” Beijing, China, September 2003 IEEE International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC’03)

[9]. H. Singh and S. Singh. "SmartAloha for Multi-hop Wireless Networks" ACM/Kluwer Journal on Mobile Networks and Applications (MONET), 2005 www.cs.pdx.edu/singh/ftp/harkirat monet04.pdf

[10]. M. O. Rabin. "Efficient Dispersal of Information for Security, Load Balancing, and Fault Tolerance". Journal of the ACM, 36(2):335–348, April 1989.

[11]. W. Lou, W. Liu, Y. Fang, "SPREAD: Improving network security by multipath routing", IEEE Milcom'03, Boston, MA, Oct 2003

[12]. A. Shamir. "How to Share a Secret" Communications of the ACM, 22(11):612– 613, November 1979.