International Journal of Current Trends in Engineering & Technology
ISSN: 2395-3152
Volume: 02, Issue: 02 (MAR-APR, 2016)

Enhancing MSF for Mobile Ad Hoc Network Security Though Active Handshaking & Multipath

Nitika Singh
PhD. Scholar Department of CSE
RKDF, Bhopal, India
singhinitika@gmail.com

Prof. Sharad Gangale
HOD Department of CSE
RKDF, Bhopal, India
sharadgangele@gmail.com

Abstract:--An ad hoc network is an automatically generated network of wireless links connecting mobile nodes. The mobile nodes can communicate without an infrastructure. They form a different topology, where the nodes play the role of routers and are free to move in a network. 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. It seems to be more challenging of in wireless networks. Existing research carried out provides authentication, confidentiality, availability, and secure routing and intrusion detection in ad hoc networks. Ad hoc network characteristics should be taken into consideration to design efficient data security along its path of transmission. Recently, some solutions are proposed to provide authentication, confidentiality, availability, secure routing and intrusion detection in ad hoc networks. Implementing security through encryption algorithm applicable at every node in such a dynamically changing network is a hard task. In this study, we focus on improving point to point data transfer using multipath routing, node to node security through encryption and handshaking of nodes. Through this process security is provided against eavesdropping, active and passive security attack and jamming using MSF (Multipath Security Framework). Indeed, we take advantage of the existence of multiple paths between nodes in an ad hoc network to increase the confidentiality and robustness of transmitted data. In our approach the original message is split into shares that are encrypted and combined then transmitted along different 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.

Keywords:- MANET, MSF, DoS, SDMP.

I. INTRODUCTION

Mobile ad hoc networks (MANET) have been gaining popularity because of availability of low cost mobile devices and its ability to provide instant wireless networking capabilities where implementation of wired network is not possible or costly. MANET is a collection of mobile node with routing capabilities and connected with wireless link. Mobile node can directly communicate to each other if they fall in the radio coverage range of each other. In order to forward the packet to the nodes which are beyond the coverage range, MANET uses the concept of multi hop communication. Nodes in the MANET are free to move, which dynamically changes the topology of the network. It does not require any expensive infrastructure to support the mobility. Creating the Ad hoc networks is possible where implementation of infrastructure is not possible or expensive. In MANET, security depends on several parameters (authentication, confidentiality, integrity, non-repudiation and availability) [1]. 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 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. We can classify these attacks into two kinds: passive and active attacks. Other attacks are Black hole attack, Routing Table overflow attack, Sleep Derivation attack, Location disclosure attack and DOS attack. In our work, we have proposed a new framework named as MSF (Multipath Security Framework), it tries to provide an effective solution to native security problems of MANET such as jamming attack, malicious node, active and passive attack and eavesdropping. In MSF, data are divided into sub parts called packet. Headers are added and then full packed is encrypted before transmission. Each packet is transmitted across different network paths which are dynamically selected. There is handshaking between the nodes to provide additional security. The motivation of proposed MSF in multipath routing protocol is to divide the initial message into parts then to encrypt and combine these parts by pairs. Then use 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 using MSF between the sender and the receiver. In our solution, 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.

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, secure routing protocols [2], preventing traffic analysis, and so on [3]. An important aspect of ad hoc network security is routing security. The Secure Routing Protocol (SRP) presented in [4, 5, 6, 7] counters malicious behavior that targets the discovery of topological information. SRP provides correct routing information Multipath routing allows the establishment of multiple paths between a single source and single destination node. Multipath routing has I been explored in several different contexts [12].Some of these schemes are characterized by the existence of a central authority, whereas others follow a self-organized approach. In this context, either some [10] or all [11] network nodes take part in issuing and verifying certificates. This is done to strengthen the protocol's resilience against attacks. A lot of work in the field has been done in mobility-based schemes that take advantage of nodes' mobility to facilitate the key exchange and trust establishment [12]. In these cases, two nodes establish security association between each other by means of secure side channel communication or physical contact. Multi-path routing has been extensively studied in a wired network context for aggregating bandwidth, reducing blocking probability, and increasing the fault tolerance, etc. [8].however, the shared wireless channel has a significant impact on the performance of multi-path routing [9].

III. Multipath Security Framework (MSF)

3.1 Multi-path Routing Topology

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 frames at MAC layer and the authentication of the terminals, a mechanism of discovering the topology of the network is available, and the protocol uses a routing protocol supporting multi-path routing and supports MSF.

3.2 Multiple path message Transmission

With the knowledge of network topology the proposed security model will use n routes (the message will be divided into n-1 shares). One path is used for signaling, 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. Therefore the proposed data security multi-path protocol should have at least 4 links.

3.3 Algorithm for Multi-path message transmission

The expressions used to describe the multi-path parted message transmission algorithm are described below:- m: message to be sent securely between A and B using multipath security framework . Dividing m into n - 1 parts gives: P (m) = {c1, c2… cn-1}. TP (ntwk): Function invoked periodically to discover topology of the ad hoc network. It returns true if modifications in topology exists, otherwise it returns false. Frequency: Represents the frequency of topology refreshing. N(A, B): number of links between A and B in MSF n: is an integer; 4<= 4 <= N(A, B). The original message m is divided into (n - 1) shares; each of them has a unique identifier. The protocol generates a path numbers of appropriate message parts to be sent on the signaling channel. The path numbers assigned for the message parts are selected randomly and sent at appropriate paths of multi-path routing protocol in MSF next message transmission different paths are used for parted messages which usually generated through pseudo random model. The message share will be transmitted in plain text the final part is sent in plain text on one of the n paths. It will be the start point for receiver to find other parts. Concerning the manner of dividing messages, a channel coding approach called Diversity Coding is used to recover from link failures. Finally combine, the n - 1 parts of m in pairs using pseudo random operation related to final path. On the nth link, which is considered as signaling channel, send values of pseudo random number and number of path in which message parts are transmitted.

3.4 Encryption of Messages in the multiple paths

The message parts on every data channel are sent encrypted by WPA to reinforce confidentiality. The chosen WPA for encryption in the proposed simulation provides efficient security to be imbibed in the multi-path routing protocol. This gives a two layer security to the data confidentiality. Combination of SDMP with WPA is performed to its perfection in terms of security and transmission efficiency. 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. Even if an attacker succeeds to obtain one part or more of the transmitted message, the probability of reconstructing the message is low. The attacker must have all the parts. This means, that he/she has to eavesdrop on all used paths, or should be near A or B. Furthermore, he/she should be informed about our combining function and be able to decrypt the WPA encoding. SDMP is deployed in an ad hoc network by introducing only software modifications.

3.5 Trust Establishment

When a node does not have valid security associations with other nodes, it executes a simple hello protocol,

with a period of TH seconds, in order to discover nodes located within its transmission range. If neighbors are detected, the trust establishment handshake is performed. When the security association is established, it is tagged with expiration time, after which it is considered invalid. The lifetime TL of each trust relationship is fixed for every node in the network. Every node maintains a list of nodes that it trusts and the corresponding time limits assigned to each trust relationship. During the neighbor discovery mechanism, a node broadcasts a HELLO message and waits for an acknowledgement (ACK-HELLO) indicating the existence of a node in its vicinity. None of these messages are encrypted, as they do not contain any sensitive information. Every node can reply to a HELLO message, even an adversary, but then it will have to prove its security credentials during the core trust establishment stage that begins upon the reception of the first ACK-HELLO packet. Any ACK-HELLO packets that may arrive later are discarded. Having discovered a neighbor, the actual trust establishment handshake between the two nodes is performed. The node u initiating the whole trust establishment process sends a JOIN packet containing its public key to the node v encrypted with the network-wide authority key that is preconfigured with. Node v decrypts the message with the same authority key and replies with a corresponding message encrypted by the same authority key. We will refer to this reply message as an ACCEPT message. In the ACCEPT message, node v includes apart from its own public key the information about the trust relationships with other nodes along with their time limits and public keys. Thus node u by establishing security association with node v, becomes member of the general secure overlay network where every node is trusted with all the others. The ACCEPT packet is then broadcasted to all nodes in the secure overlay network in a secure way since each transmission is made between trust related nodes. At each transmission between trusted nodes public key cryptography is used. The network-wide authority key is only used in the core trust establishment phase. In order to avoid using any information from the routing layer, a controlled flooding mechanism is performed ensuring, by means of sequence numbers, that each node forwards each ACCEPT packet only once. As a result, all nodes of the secure overlay eventually share the same information regarding which nodes and until when, can be trusted.

TABLE 1

	Proposed protocol	[10]	[11]	[14]	[15]	[13]	[13]	[16]
Authority based	Yes	Yes	Yes	Yes	No	No	Yes	No
Preconfigured keys	Yes	Yes	Yes	Yes	No	No	Yes	No
Key update mechanism	Yes	Yes	Yes	No	Yes	No	No	No
Threshold cryptography	Yes	Yes	Yes	Yes	No	No	No	No
Advanced cryptography	No	No	No	No	Yes	No	No	Yes
Secure side-channel	No	No	No	No	No	Yes	No	No

3.6 Establishment of Multipath Routes in MSF

The success of multipath selection necessitates two components, namely: 1) a metric that can accurately reflect failure correlation between different paths, and 2) a selection algorithm that can effectively leverage the metric to rule out failure-correlated paths from being selected together. We present a mechanism which can not only evaluate individual path availability, but can also derive a multipath availability metric even in the presence of failure correlation between links. Then, we sketch how our mechanism helps to select multiple paths based on the derived availability metric. We use the following standard notations: "∧" is the logical AND bit-operation; "∨" stands for the logical OR bit operation; "|X|" operation returns the cardinality of the set X; and "||X||" operation returns the norm of the vector X.

a) MSF History Vector (MHV)

Given the increasing possibility of cross-platform interference and jamming in wireless networks, as well as the overwhelming complexity of the wireless propagation environment that a wireless network relies on, it is

International Journal of Current Trends in Engineering & Technology
ISSN: 2395-3152
Volume: 02, Issue: 02 (MAR-APR, 2016)

difficult (if not impossible) to precisely predict analyze the correlation between different paths. To bypass such complexity while still exploring the failure correlation between different paths, we propose a mechanism called an MHV [17], to record path availability histories, from which the failure correlation between different paths can be learned. We first define an MHV on a per-link basis, from which path (multipath) availability can be then easily derived. One natural metric to determine the availability of a wireless link is the Packet Delivery Ratio (PDR), i.e., the percentage of packets successfully delivered over the link. Recording the PDR time series directly requires at least 1 byte for each data point, and calculating the aggregated PDR of a path requires multiplication To store and compute availability history efficiently, we utilize a binary vector for recording, and bitwise operations for calculating path availability. In particular, we map a PDR to a 0-1 value, where "1" corresponds to the time instant when the link is available (acceptable PDR), while "0" corresponds to the time instant when the link is unavailable (unacceptable PDR). A threshold γ_o is predefined to determine whether a PDR is acceptable, and γ_o should be sufficiently high to ensure acceptable end-to-end PDRs. Furthermore, we divide time into epochs with a fixed duration. At the lth epoch, let $PDR^l_{i\_}$ be the average PDR between nodes ì and j, then the availability record of the link between nodes i and j at the *l*th. epoch is $r^l_{i\_}$ =1 if { $PDR^l_{i\_} \geq \gamma_o$, otherwise: 0. The MHV of this link for e epochs is Aij=[$r^1_{i\_}$; $r^2_{i\_}$ . . . $r_{i\_}$]. To facilitate observation, we depict an MHV as a continuous line and illustrate an example of converting the PDR into the MHV with γ_o being 0.6 in Fig.1; except for Epoch 9, the availability of other epochs is "1." So far, MHV is used to characterize individual links. Now, we present how to derive an MHV for an entire path consisting of concatenating links or sub paths, using the following series combination operation.

b) MHV of one path

The MHV of a complete path is computed as the logical bitwise AND of all MHVs of the links or sub paths. The MHV of path pi can be formulated as $A=a_{I1I2}\wedge a_{aI2I3}\wedge\ldots\wedge a_{IqIq+1}$. Where Iq is the qth node ID on the path p_i. For example, Path-1, shown in Fig. 2, consists of links 1 ! 2 ! 3 ! 8. Fig. 5 illustrates the series combination for calculating its MHV. The top three lines present the MHVs of links 1 ! 2; 2 ! 3; and 3 ! 8, and the fourth line is the MHV of Path-1, computed as the bitwise AND of the first three MHVs.

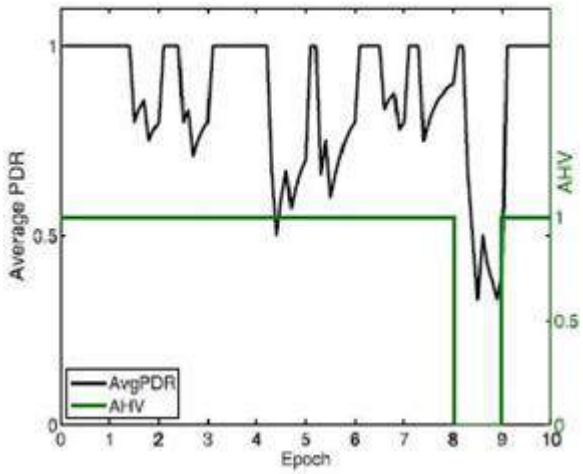

Figure 1 an illustration of converting PDR to AHV for the link 1 to 2

c) MHV of multiple paths

Recall that in multipath routing, we aim at selecting multiple paths that provide the highest multipath availability; thus, we derive the AHV of a given set of k paths using the following parallel combination operation. Let M be the set of k paths between a source-destination pair. The MHV of M is computed as the logical bitwise OR of all MHVs of the paths, denoted as $A_M=A_1 \vee A_2 \vee A_3 \vee \ldots \vee A_k$. Given example shows of the MHVs of three paths along with the combined MHV of Path-1 and Path-3, obtained by a logical bitwise OR of the Path-1 and Path-3's MHVs.

d)Multipath availability metric θ

From the availability history carried by MHVs, we can

International Journal of Current Trends in Engineering & Technology
ISSN: 2395-3152
Volume: 02, Issue: 02 (MAR-APR, 2016)

infer that two paths are highly correlated if they tend to fail at the same time, and vice-versa. To facilitate selecting failure-independent routing paths, we define an availability metric θ, which is computed as the number of 1-epochs (i.e., availability bit equals "1" in that epoch) in the MHV of multiple paths between a source-destination pair. Specifically, the availability of a multipath set M is $\theta(M)=||A_M||$. Consider the example shown in Fig. 3, θ of the set of Path-1 and Path-2 is 8.

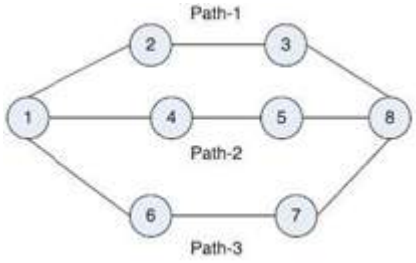

Figure 2 simplified topology of a wireless network with three paths

3.7 Multipath Selection

The goal of our multipath selection scheme is to select k MHVs that can produce the largest θ, to ensure that failure correlated paths are bound to be less likely chosen together. Formally, given the set H containing h candidate paths, the multipath selection problem can be defined as the following Definition 1: Maximize θ(M) subject to $|M| \leq k$, $M \subseteq H$.

a)Multipath selection framework

Obtaining the optimal M in MSF containing k paths encounters two challenges. First, the multipath selection problem in Definition 1 is NP-complete, according to our prior work [36]. Second, a huge number of possible paths may exist between nodes in a multihop wireless network. Consider a 2-by-2 grid network with each node connected with the other three nodes, as shown in Fig. 6. Five disjoint, loop-free paths exist from 1 to 4: 1 ! 4, 1 ! 3 ! 4, 1 ! 2 ! 4, 1 ! 2 ! 3 ! 4, 1 ! 3 !2 ! 4. It is foreseeable that as the number of nodes increases, the number of paths will increase exponentially.

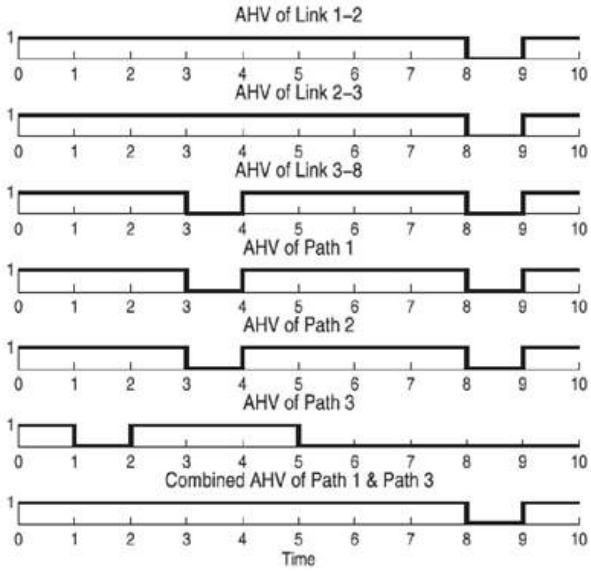

Fig.3.The MHV for the network in figure 5.

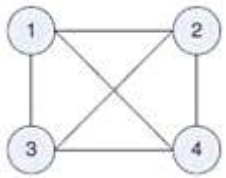

figure 4 A 2 by 2 network

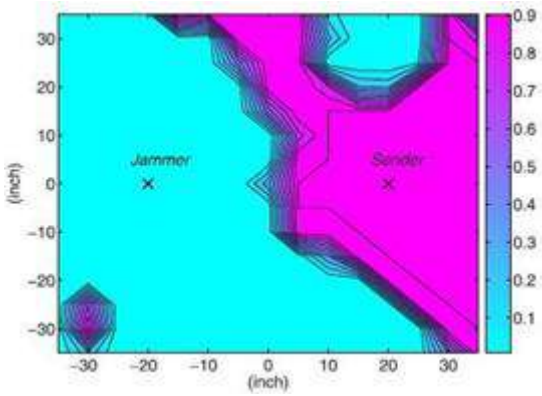

Fig.5. PDR contours of a sender located at (20,0) in the presence of a jammer located (-20,0)To illustrate irregularity of jam in the real system.

VI. CONCLUSION

In this paper, we have addressed the problem of multipath selection with the goal of improving data confidentiality jamming resilience, eavesdropping, passive and active attack in wireless networks problem by exploiting a very important ad hoc network characteristic, which is the existence of multiple paths between nodes. Our key insight is to select multiple

paths Our protocol is strongly based on multipath routing DSA and MSF characteristics of ad hoc networks and uses a route selection based on security costs. Using MSF that are unlikely to fail concurrently, based on the knowledge of paths' availability histories. The availability histories of paths are efficiently recorded and calculated via multipath history vectors.

REFERENCES

[1]. 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.

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

[4]. Yih-Chun Hu, A. Perring, A survey of secure wireless ad hoc routing, IEEE Security and Privacy 2 (3) (2004).

[5]. 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.

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

[7]. 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.

[8]. 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 .

[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]. Z. Zhou, Z.J. Haas, Securing ad hoc networks, IEEE Network **13** (1999), no. 6, 24–30 .

[11]. J. Kong, P. Zerfos, H. Luo, S. Lu, L. Zhang, Providing robust and ubiquitous security support for mobile ad-hoc networks, Int'l Conf. on Network Protocols, pp. 251–260, 2001. 12.P. Papadimitratos and Z. Haas, "Secure Routing for Mobile Ad Hoc Networks," Proc. SCS Comm. Networks and Distributed Systems Modeling and Simulation Conference (CNDS '02), 2002.

[12]. 13.S.Capkun, J.-P. HUbaux, L. Buttyan, Mobility helps security in ad hoc networks, Proc. of the Int'l Symposia on Mobile Ad Hoc Networking and Computing, pp. 46–56, 2003.

[13]. A. Khalili, J. Katz, W.A. Arbaugh, Toward secure key distribution in truly ad-hoc networks, Symposium On Applications and the Internet Workshops, pp. 342–346, 2003.

[14]. J. van der Merwe, D. Dawoud, S. McDonald, Fully self-organized peer-to-peer key management for mobile ad hoc networks, Proc. of the ACM Workshop on Wireless Security, pp. 21–30, 2005.

[15]. M. Cagalj, S. Capkun, J.-P. Hubaux, Key agreement in peer-to-peer wireless networks, IEEE Special Issues on Cryptography and Security, 2006 .

[16]. X. Zhang and A. Perrig, "Correlation-Resilient Path Selection for Multi-Path Routing," Proc. IEEE Globecom, 2010.