ISSN:0975-9646
K.P. Manikandan et al, / (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 2 (3) , 2011, 1007-1011

# A Cross Layered Architecture and Its Proposed Security Mechanism to Lessen Attacks Vulnerability in Mobile Ad Hoc Networks

K.P.Manikandan,[1]R.Satyaprasad[2] K.Rajasekhararao[3]
[1]*Chirala Engineering College,India*
[2]*Achariya Nagarjuna University,India*
[3] *KL University,India*

***Abstract-*** **A Mobile Ad Hoc Network (MANET) is a network that does not have underlying infrastructure. Hosts in MANET are connected by wireless links with multi-hop communication. The nodes in MANET themselves are responsible for dynamically discovering other nodes to communicate. Although the ongoing trend is to adopt ad hoc networks for commercial uses due to their certain unique properties, the main challenge is the vulnerability to security attacks. A number of challenges like open peer-to-peer network architecture, stringent resource constraints, shared wireless medium, dynamic network topology etc. are posed in MANET. Besides, MANET's highly self-organized and self-maintained attributes increase its vulnerability to be attacked. Examples of attacks include Denial of Service (DoS), node impersonation, information disclosure, message injection, Continuous Channel Access (Exhaustion), routing disruptions, Sinkhole, Wormhole, and Node Capture. These attacks can happen at any layer in network protocol stack. Thus, it is essential to provide security services in order to overcome those threats. This paper presents a cross-layer design approach for MANET in achieving security and QoS.**

***Keywords: MANET, Cross Layered Design, Security Services, LIA***

## I. INTRODUCTION

### A. *Mobile Ad-hoc Networks*

A mobile ad-hoc network (MANET) is a temporary infrastructure less multi-hop wireless network in which the nodes can move arbitrarily. Such networks extend the limited wireless transmission range of each node by multi-hop packet forwarding, thus, well suited for the scenarios in which pre deployed infrastructure support is not available. In an ad hoc network, there is no fixed infrastructure such as base stations or mobile switching centers. Mobile nodes that are within each other's radio range communicate directly via wireless links, while those that are far apart rely on other nodes to relay messages as routers. Node mobility in an ad hoc network causes frequent changes of the network topology. Mobile ad hoc networks are finding ever increasing application in both military and civilian scenarios due to their self-organizing, self-configuring capabilities.

### B. *Security Threats in MANETS*

An ad hoc network can be attacked from any direction at any node which is different from the fixed hardwired networks with physical protection at firewall and gateways. Altogether it denotes that every node should be equipped to meet an attacker directly or indirectly. Malicious attack can be initiated from both inside and outside of the network. Tracking a specific node is difficult in large ad hoc networks and hence, it is more dangerous and much difficult to detect the attacks from an affected node. Altogether it denotes that every node should be prepared to work in a way that it should not trust on any node immediately.

Distributed architecture should be applied in order to achieve high availability. This is because if the central entity is used in the security solution, it causes serious attack on the entire network when the centralized entity gets affected.

This paper describes an algorithm that helps MANET routing in two ways. First, it provides a metric that by its nature warns of the possibility that links can break. This metric, which can be considered a link stability index, accumulates at each node to form a path stability index. Therefore, the algorithm enables intermediate nodes to balance stability of the route with end-to-end delay. Its principle is simple: intermediate nodes must wait before they re-broadcast a request they just picked up from a neighbor. This waiting mechanism has, in turn, two advantages. First, in case a better link comes along, there is no need for re-broadcast. This reduces overhead of redundant broadcasts. Second, by using a simple waiting mechanism that depends on link stability, end-to-end delay reduces.

## II. BASICS OF CROSS-LAYER DESIGN

### A. *Definition*

To fully optimize wireless broadband networks, both the challenges from the physical medium and the QoS-demands from the applications have to be taken into account. Rate, power and coding at the physical layer can be adapted to meet the requirements of the applications given the current channel and network conditions. Knowledge has to be shared between (all) layers to obtain the highest possible adaptively.

The algorithm proposed here uses cross-layer design concepts. This approach, in its general form, is depicted in Figure.1 and enables protocol layers to work together. The purpose of cross-layer cooperation is adaptation to channel conditions. Layer 1, the physical layer or PHY, measures the quality of a radio link and forms the metric CQI, the Channel Quality Indicator. Many methods to measure CQI are available, mostly based on measuring the signal-to-noise ratio in a link. The CQI, once used within PHY, enables adaptive modulation (and coding). It helps the transmitter and the receiver to decide which modulation and coding scheme works best for the link within a particular time-frame. Layer 2, the media access control (or MAC) layer is in charge of scheduling access to the channel by the users. MAC can benefit from CQI measurements to figure out which users are best scheduled now (if their channels are good) or later. Layer 3, or the network layer, is responsible for routing. The concept of using PHY metrics for adaptive routing is not new. In fact, significant results based on physical layer constraints have been reported in [7] and [8]. What is new, and the intention of this paper, is a simple and effective method for mapping physical layer measurements to link stability (or rather instability) and then including link stability in routing algorithms. Architecture in tackling security challenges mobile ad hoc networks are facing.

This paper is discussed the present security architecture in a layered view and analyzes the reasoning for such security architecture. This security architecture can be used as a frame work when designing system security for ad hoc networks. A key element to the proposed framework is that it will combine well-known cryptographic mechanisms (such as digital certificates and signatures), with different sources of identification information. This information comes in the form of attributes describing physical node characteristics, much like the biometrical characteristics examined during human identification and authentication.

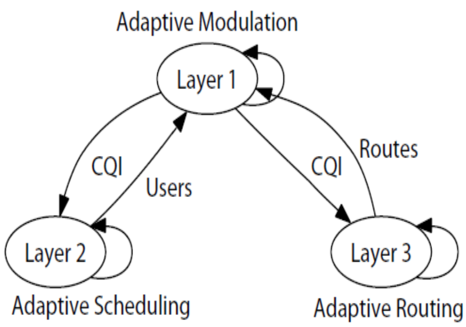


*Fig. 1: Outline of Cross-Layer Design*

## III. CROSS-LAYER SECURITY SERVICES

There are advantages to using this cross-layer architecture for security in MANET networks. By taking metrics from the security services at one layer, such as from authentication systems and intrusion detection systems (IDS), operations at other layers can be made more secure or optimised. For example, authentication and intrusion detection systems operating at the application layer can provide real-time attack profiles into an integrated cross-layer security service. The results (metric or metrics) can then be used by the lower layers to improve their efficiency (they don't have to calculate the security metric themselves) and robustness (security is derived from the multiple methods used across the various communication layers). While this frame work may increase the complexity and internal processing within a node (in order to integrate multiple functions), it should reduce the communication requirements between nodes (since confirmation with neighbouring nodes is no longer as critical). This is especially beneficial to networks where bandwidth is limited. Some potential security services that could be integrated using this framework are described below.

### A. *Intrusion Detection*

Intrusion detection systems (IDS) are employed to determine when the network is being subjected to a network or application layer attack. Such systems are one of the more effective ways to counter, for example, masquerade threats [2]. An IDS can benefit from the establishment of a "trust model", for example, to distinguish among friends, acquaintances and adversaries. An intrusion detection or similar behavioural analysis engine can be charged with monitoring neighbours. In tactical networks, the IDS will likely need to be distributed rather than centralised. This leads to a "watchdog" approach where nodes monitor and analyse the behaviour of their local neighbours.

Lessons can be drawn from existing work in the area of Byzantine routing, including consensus algorithms to eliminate falsified information, which can make the system more robust. There are also various methods of establishing trusted routes based on hash chains and digital signatures, but these methods may prove to have too much overhead and consume too much bandwidth to be applicable to the networks [3]. In fact, many of the security overlays proposed in the area of ad hoc networking suffer from overhead issues or complicate the communication protocols such that interoperability among coalition partners could be threatened if different security solutions are employed. Research is being conducted that allows for the provision of security services such as intrusion detection and authentication in mobile ad hoc networks without relying on additional messaging [1], however it is often the case that detection of an attack at one layer requires mitigation techniques be applied at another. For example, if a Sybil attack, in which a node claims several identities (Masquerade), is detected at the application layer, the response may be to block all traffic coming from the attack's location by eliminating the route from the routing table [4].

### B. *Frequency Hopping*

Frequency hopping is a well known physical layer defence against frequency jamming. The radio transmits on a set of frequencies in a pre-determined sequence followed by all corresponding nodes in the network. By using frequency hopping, a wider range of the spectrum is used making it more difficult for an adversary to transmit sufficient energy within that band to interrupt the demodulation at the receiver. One of the potential benefits of cross-layer enabling the physical layer is the use of application level characteristics to understand when and to what extent jamming is expected to be a problem. In a time of transmission of critical information, or when the node is in a physical location known to be prone to jamming, the rate and range of frequency hopping can be tuned to the application level requirements based on a security policy. That is, application layer analysis can be used to dynamically modify physical layer attributes.

### C. *Distributed Authentication*

For security services in a distributed network, threshold cryptography is generally used to let some or all network nodes share a network master key and collaboratively provide security services such as issuing and refreshing private keys. In a network with N nodes, a group of n special nodes is capable of generating partial certificates using their shares of the certificate signing key. A valid certificate can be obtained by combining k such partial certificates, which is called (k, n)-threshold cryptography.

In MANETs, identity (ID)-based cryptography with threshold cryptography is a popular approach for the security design because key management is simpler than that of public key infrastructure (PKI). In threshold schemes, the network can tolerate the compromise of up to (k −1) shareholders. The security of the whole network is breached when a threshold number of shareholders (k) are compromised. Therefore, the optimal selection of nodes in threshold cryptography should be carefully investigated. However, most previous work for key management in this framework concentrates on the protocols and structures. Consequently, how to optimally conduct node selection in ID-based cryptography with threshold secret sharing is largely ignored. In [5], a distributed scheme based on the stochastic multi-arm bandit formulation is proposed. The proposed scheme can select the best nodes for reconstructing the full secret taking into account the security conditions to minimise the overall threat posed to the network. We can utilize the information obtained from the Metric Store for node selection. For example, we can assign a weight value for a node based on the information from Metric Store. If a node has high security, it may have higher weight. We then conduct the node selection process considering the weights to achieve higher security.

## IV. LIGHT WEIGHT INTEGRATED AUTHENTICATION

In order to further validate our architecture, this section describes a security problem for tactical networks and details how a solution can be augmented using our cross-layer architecture. We base the case study on previous work on the lightweight integrated authentication (LIA) scheme in MANETs [6]. Authentication is an important element of network security because it is the first step toward prevention of, and guarding against, unauthorized access to network resources and sensitive information. We hope to efficiently utilize the authentication results for other security services such as secure routing through the cross-layer scheme. LIA is summarised below, followed by a discussion of how it could be adapted to and benefit from a cross-layer design such as the one detailed in this paper.

### *A. Overview of LIA*

In the LIA scheme, each node maintains a trust table which is a fusion of security information of all the neighbouring network nodes. It is first established based on authentication and then kept updated based on any available intrusion detection systems (IDSs) and the key self-revocation mechanism of LIA. The value of the trust field can be thought of as raw data – its utilisation is application dependent [4].

The details of managing the trust table are provided as follows:

*Step 1: Bootstrapping*: As described by McGrath et. al. [9], LIA uses an off-line PKG that generates Identity Based Encryption (IBE) private keys for all devices based on their unique identities. This is feasible in tactical networks because before deployment, users with their devices have to report to a command post where the Private Key Generator (PKG) could be located.

*Step 2: Pre-authentication*: Using its private key and the public key of its recipient node, every node can compute its pair wise symmetric key for authentication with the recipient. This key is the same for both nodes because of the bi linearity property of IBE [10].

*Step 3: Credential establishment:* A pair wise symmetric key is communicated between the two nodes. The symmetric key is encrypted for confidentiality using the public key of the recipient, and signed for authentication using the private key of the sender.

*Step 4: Authentication*: Mutual authentication is performed when the two nodes compare their pair-wise symmetric keys. This key can also be used as session key for securing the data communications. A trust table is then built to store the trust values of its neighbours. The value of the trust field can be either Boolean (e.g., zero or one) or multi-level (e.g., zero, low, medium, high). Once node i is authenticated by node j, the trust value of node i can be set to one in node j's Trust Table. When the public key of node i is revoked, the trust value of node i can be set to zero in node j's Trust Table. The Trusted routes could then be established through authenticated nodes with non-zero trust values. Security policy can define if a message can be routed through all available routes or only trusted routes

*Step 5: Monitoring*: This is accomplished through continuous user-to-device authentication with IDS. User and device are assumed to be tightly coupled in a tactical operation. When user-to-device authentication fails, it implies that the device is not in the hands of a legitimate user. This event triggers revocation of the public key of the device. We recommend performing user-to-device authentication through wearable biometric sensors because they have the following properties: 1) direct user binding, 2) non-disruptive re-authentication, 3) inherent liveliness detection [11].

*Step 6: Revocation*: LIA introduces a self-revocation mechanism by leveraging the integration of user-to-device and device-to-network authentication. This concept is illustrated in Figure 2. Once the user-to-device authentication fails, which implies the compromise of the device, the device informs the neighbouring nodes using a Good Bye message. The node will then be excluded from the trusted routes of its neighbours. The Good Bye message is similar to a Hello message in a proactive routing protocol such as the Optimised

Link State Routing protocol (OLSR) [12] but it performs a Good Bye-type operation, excluding the sender from its neighbours' trusted routes. The existing message handlers in OLSR can be re-used to process this message to implement the Distributed Revocation Authority and to propagate the Good Bye message to neighbouring nodes' Trust Tables.

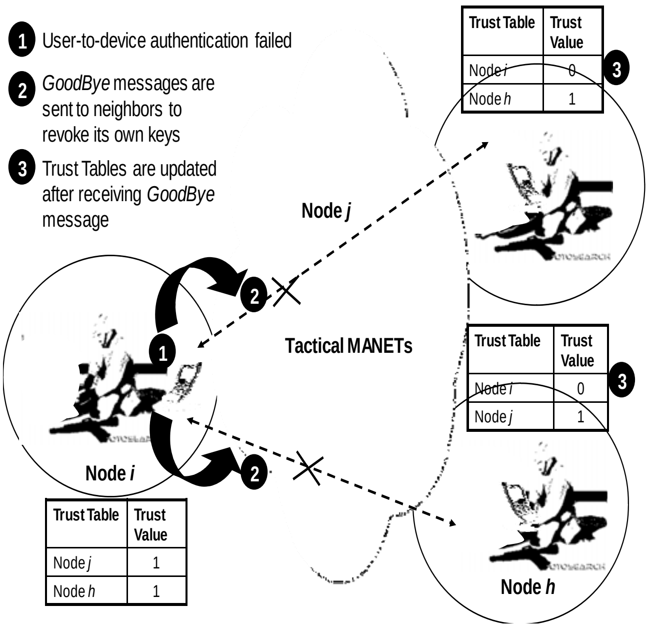


**Fig. 2: LIA's Self-revocation Mechanism.**

In order to create a Good Bye message, LIA proposes adding a Link Type to the existing format of the Hello message indicating that the trust value of the sender should be changed to zero in the receivers' trusted routing table. The Good Bye messages must be encrypted and sent to all the neighbours as adversaries may fabricate such messages to cause public keys of uncompromised nodes to be revoked – a denial of service attack.

*B. LIA within a Cross-layered Architecture*

As mentioned in Section 4.1, the trust table can be viewed as the fusion of the security information of all network nodes. As such, it is a natural extension to allow the trust table to be a part of the Metric Store. The trust value can be set with the authentication and IDS results obtained in the application layer, results which can also be part of the Metric Store. Any layer that is interested in the trust values can subscribe to the service and access the trust table. In the following, we list 4 examples showing how 4 layers can enhance their security by utilizing the trust values.

1. At the session layer, a security policy can be defined to allow applications establish sessions with those nodes that have a minimum trust value. During a session establishment, in addition to session parameters such as IP address and port number, the trust value of a node is also communicated. The source node automatically decides whether to continue establishing a session to that destination node or not. The applications can range from e-mail, FTP, HTTP, VoIP or even a video or data session. Deploying this approach at session layer not only eliminate user intervention but also reduces the security risks while adaptively adjust to time varying security requirements.
2. At the routing layer, routing table can be built incorporating the trust values. The routing table is built based on certain routing algorithms such as OLSR [10]. The security of routing algorithms is usually addressed through cryptographic algorithms. If we could incorporate the trust values when we build the routing tables, we can more efficiently enforce certain security policies such as letting a message be routed through any available route or only through nodes with certain trust value. This feature is especially useful in coalition operations where multiple countries cooperate but with different security requirements. For example, certain encrypted messages like command and control messages for designated receivers must be routed through nodes with a minimum trust value.
3. For MAC layer, longer medium access time may be allocated to the nodes that have higher trusted value;
4. For physical layer, we can utilize the information obtained from the trust table for distributed spectrum sensing. We can increase the trustworthiness of the spectrum sensing results by assigning higher weights to the sensing results obtained from nodes with higher trust values.

There are two main advantages of using LIA within this scheme for tactical MANETs. It results in less communication overhead between nodes and it enhances the security at different layers, allowing greater flexibility in defining the security policy according to application needs.

## V. CONCLUSION

Due to the mobility and open media nature, the mobile ad hoc networks are much more prone to all kind of security risks, such as information disclosure, intrusion, or even denial of service. As a result, the security needs in the mobile ad hoc networks are much higher than those in the traditional wired networks. First we briefly introduce the basic characteristics of the mobile ad hoc network and its cross layered architecture. Because of the emergence of the concept pervasive computing, there is an increasing need for the network users to get connection with the world anytime at anywhere, which inspires the emergence of the mobile ad hoc network. However, with the convenience that the mobile ad hoc networks have brought to us, there are also increasing security threats for the mobile ad hoc network, which need to gain enough attention. In this paper, we discuss the cross layered design attacks vulnerability and its defensive methods such as Intrusion detection, frequency hopping, distributed authentication and LIA to provide better services against DoS. Even though, these Detection mechanism can be enhanced with any type of attacks that utilized with cross-layered approach. It can also be enhanced on cross layered based IDS using hybrid approach for both misuse and anomaly detection with effective decision making to reduce the false alarm rate.

## REFERENCES


[1] L. Romdhani and C. Bonnet, “Achieving a good trade-off between complexity and enhancement in cross-layer architectures”, in Proceedings of the 2nd International Conference on Information and Communication Technologies, 2006, pp. 2473-2478.

[2] D. Lynch et al., Providing Effective Security in Mobile Ad Hoc Networks Without Affecting Bandwidth or Interoperability, in Army Science Conference 08, 2008.

[3] Y.C. Hu and A. Perrig, A Survey of Secure Wireless Ad Hoc Routing, in IEEE Security and Privacy, 2004.

[4] F. R. Yu, H.Tang, F. Wang, V. C.M. Leung, Distributed Node Selection for Threshold Key Management with Intrusion Detection in Mobile Ad Hoc Networks, in the 2009 IEEE/IFIP International Symposium on Trusted Computing and Communications (TrustCom-09), Vancouver, Canada, August 29-31, 2009.

[5] John R. Douceur, The Sybil Attack, Revised Papers from the First International Workshop on Peer-to-Peer Systems, p.251-260, March 07-08, 2002

[6] H. Tang and M. Salmanian, Lightweight Integrated Authentication for Tactical MANETs, in International Symposium on Trusted Computing (TrustCom-08), Zhangjiajie, China, Nov. 18-21, 2008.

[7] G. Ferrari, S. A. Malvassori, M. Bragalini, and O.K. Tonguz, Physical layer-constrained routing in ad hoc wireless networks: A modified AODV protocol with power control, in Proc. Int. Workshop on Wireless Ad-hoc Networks 2005 (IWWAN 2005), London, UK, May 2005.

[8] I. Rubin and Y. Liu, Link stability models for QoS ad hoc routing algorithms, in IEEE 58th Vehicular Technology Conference (VTC), vol. 5. IEEE, 2003,pp. 3084-3088.

[9] C. McGrath, A.S. Ghazanfar and M.McLoone, Novel Authenticated Key Management Framework for Ad Hoc Network Security, in Proceedings of. ISSC 2006, Dublin, June, 2006.

[10] D. Boneh, and M. Franklin, Identity-based encryption from the Weil Pairing, in Advances in Cryptology – CRYPTO ‘2001, LNCS 2139, pp 213-229, 2001.

[11] H. Tang, M. Salmanian and Q. Xiao, Biometric-based User Authentication for Tactical Mobile ad-hoc networks, DRDC Ottawa Technical Note 2007-100, May 2007.

[12] T.Clausen and P.Jacquet Optimized Link State Routing Protocol (OLSR), IETF RFC 3626, October 2003. http://www.ietf.org/rfc/rfc3626.txt