

# A security architecture for Mobile Ad Hoc Networks

Shuyao Yu

Institute of Computing Technology,  
Computer Network Information  
Center of Chinese Academy of Sciences  
No.4 South 4th Zhong Guancun  
Road, Beijing, China, 100108  
86-0-13161674845  
shuyao@cnic.cn

Youkun Zhang

School of Software,  
Tsinghua University  
86-10-64867270  
zhangyoukun@tsinghua.org.cn

Chuck Song

Computer Network Information  
Center of Chinese Academy  
of Sciences  
No.4 South 4th Zhong Guancun  
Road Beijing, China, 100108  
86-10-62650655  
song@cnic.cn

Kai Chen

Bell Labs  
Research China  
15<sup>th</sup> floor Hangtian  
Changcheng Building  
Beijing, China, 100080  
kaichen@lucent.com

## ABSTRACT

A Mobile Ad Hoc Network (MANET) is a self-organizing, infrastructureless, multi-hop network. The wireless and distributed nature of MANETs poses security a great challenge to system designers. Most current work done to resolve security problems in MANETs is limited in some specific aspects of system security, none of the previous work propose solutions from a system architectural view. In this paper, we propose a five-layer security architecture for mobile ad hoc networks. A general description of functionalities in each layer is given and we analyze the security mechanisms in military applications in the scope of the proposed security architecture.

## Keywords

Mobile Ad Hoc Network, Security, Authentication, Security Architecture.

## 1. INTRODUCTION

A Mobile Ad Hoc Network (MANET) is a network consisting of a collection of nodes capable of communicating with each other without help from a network infrastructure. Applications of MANETs include the battlefield applications, rescue work, as well as civilian applications like an outdoor meeting, or an ad-hoc classroom. With the increasing number of applications to harness the advantages of Ad Hoc Networks, more concerns arise for security issues in MANETs.

The nature of ad hoc networks poses a great challenge to system security designers due to the following reasons: *firstly*, the wireless network is more susceptible to attacks ranging from passive eavesdropping to active interfering; *secondly*, the lack of an online CA or Trusted Third Party adds the difficulty to deploy security mechanisms; *thirdly*, mobile devices tend to have limited power consumption and computation capabilities which makes it more vulnerable to Denial of Service attacks and incapable to execute computation-heavy algorithms like public key algorithms; *fourthly*, in MANETs, there are more probabilities for trusted node being compromised and then being used by adversary to launch attacks on networks, in another word, we need to consider both insider attacks and outsider attacks in mobile ad hoc networks, in which insider attacks are more difficult to deal with; *finally*, node mobility enforces frequent networking reconfiguration which creates more chances for attacks, for example, it is difficult to distinguish between stale routing

*The space is reserved for copyright.*

information and faked routing information.

There are five main security services for MANETs: *authentication*, *confidentiality*, *integrity*, *non-repudiation*, *availability*. *Authentication* means the correct identity known to communicating partner; *Confidentiality* means certain message information is kept secure from unauthorized party; *integrity* means message is unaltered during the communication; *non-repudiation* means the origin of a message cannot deny having sent the message; *availability* means the normal service provision in face of all kinds of attacks. Among all the security services, authentication is probably the most complex and important issue in MANETs since it is the bootstrap of the whole security system. Without knowing exactly who you are talking with, it is worthless to protect your data from being read or altered. Once authentication is achieved in MANET, confidentiality is a matter of encrypting the session using whatever key material the communicating party agree on. Note that these security services may be provided singly or in combination.

In this paper, we propose a security architecture from a layered view, then the functionalities of each layer is described. We further analyze the application of the proposed security architecture in military applications.

The remainder of this paper is organized as follows: Section 2 introduces related work to security in MANETs; the proposed security architecture is presented in Section 3; Section 4 analyzes the application of the proposed security architecture in military scenarios; Conclusion is made in Section 5 and Section 6 marks the acknowledgements.

## 2. RELATED WORK

We classify related work to ad hoc network security into the following three categories:

- Providing basic security infrastructure: MANET is a network without any basic infrastructure, hence there is no trust infrastructure like PKI for all the participating nodes in MANETs. The first step to establish a security system is to setup the basic security infrastructure and establish security associations between communicating nodes.
- Secure routing: In MANETs, every node participates in the routing activities in MANETs. There are two concepts in secure routing here: one is exchanging routing information to keep the network connected and the other involves secure data packet forwarding.
- Misbehavior/Intrusion detection and response: The wireless and mobility nature of ad hoc networks makes it vulnerable to intrusions and misbehaviors than in wired counterpart. Note that misbehaviors and intrusion are different both in the motivations and in the degree of damage, while intrusion means an attack launched by adversaries which may cause

severe consequences, misbehavior usually means “selfish” nodes that do not contribute their resources to the maintenance of network connectivity for the reasons like saving its battery life, CPU or memory, hence, can cause less damage but inefficient networking.

[8] presents a distributed public-key management service for ad hoc networks. The MANET network has a system public/private key pair PK/SK, while the public key is known to all the nodes, the secret key SK is divided into  $n$  shares using an  $(n, t+1)$  threshold cryptography. Every node entering the network should obtain a certificate which is signed collectively by any  $t+1$  servers from the  $n$  servers ( $t < n$ ). The application of threshold cryptography  $(n, t+1)$  assures that the system can tolerate up to  $t$  nodes being compromised. And any node that can find  $t+1$  servers in its neighborhood to sign the signature be authenticated to the system. The paper also proposed proactive share refreshing. The paper requires a dealer to initialize the system and after self-initialization the dealer is no longer needed and the trust relationship between nodes are managed by the servers cooperatively.

[8] is further developed by [5], while in [8] only servers can cooperatively sign a signature, [5] distributes the server role to all the nodes in the network, any node which can obtain a certificate signed by any  $t$  nodes can be authenticated in the network.

There are also some work using PGP-like method [6][12][14] to construct the trust infrastructure for MANETs. Each node signs other nodes' certificates based on certain policy. Each user maintains a local certificate repository that contains a limited number of certificates selected by the user based on some algorithms. A node accepts a certificate if the certificate bears a certificate chain from the nodes that are already known to be trustworthy. While this is applicable to small-world situation, it does not scale well to a relatively large network where nodes are mobile.

There is also an interesting paper [3] concerning the trust model issue. [3] proposes an appropriate model for a well defined hierarchy of trust relationships. The duckling will take the first entity that sends it a secret key as its mother and obey all the command from the mother after they reach a security association. The security association is broken when the duckling dies and gains a rebirth when another mother appears. While this model works well for large and hierarchical networks, it can not be easily applied in general other scenarios.

Routing is more vulnerable in MANETs than in wired networks where routers are always managed by trusted parties to protect them from attacks. Thus, much of the effort in providing security for mobile ad hoc networks is spent in secure routing protocols. [1] [4] [9] [16] provide security mechanisms based on some routing protocols, like DSDV, DSR and AODV. The security mechanisms added to the existing routing protocols are constructed on the assumption that security association already exists between the communicating parties at the beginning of networking. In fact, the effort in securing routing protocols done so far should be based on certain trust infrastructure which needs to be established before secure routing protocol takes effect.

There are some end-to-end network layer solutions aiming at reliable and confidential data transmission based on certain routing protocols. [15] presents the Secure Message Transmission(SMT) protocol which can operate solely in an end-to-end manner and can operate with any underlying routing protocol which can discover multiple routes. SMT utilize multiple paths between end nodes to redundantly transmit data packets to

achieve reliability. SMT allows the reconstruction of original message with successful reception of any  $M$  out of  $N$  ( $M < N$ ) transmitted pieces. [10] and [11] bear a similar idea, while instead of focusing on reliability of data transmission as [15] does, they utilize multiple routes between communicating peers to increase the confidentiality of the transmitted data packets.

In previous work done related to intrusion/misbehavior detection and response, [13] proposed two mechanisms: *pathrater* and *watchdog* to improve throughput in the presence of nodes who agree to forward packets but fail to do so. *Watchdog* is used to identify misbehaving nodes while *pathrater* evaluates node ratings reported by all nodes and gets the result which can be as a path metric to help routing protocols avoid these misbehaving nodes.

[7] presents an approach using a currency-like mechanism called *nuggets* to stimulate end users to keep their devices turned on, to refrain from overloading the network and to thwart tampering aimed at converting the device into a “selfish” one.

[17] introduces a new intrusion detection architecture for MANETs, and presents a multi-layer integrated intrusion detection and response scheme.

None of the previous work gives solution from a system architectural view or describes the whole picture of how the building blocks of security mechanisms are combined together to fulfill the security requirement of MANETs. In Section 3 we will present our proposed security architecture.

### 3. SECURITY ARCHITECTURE FOR MANETS

As we have learned from the history of Internet attacks, security can not be considered separately after the whole infrastructure of network has been designed. As a characteristic example, IPsec is the result of lack of methodology in network security protocol design. It is not only technically complex to deploy but also with conflicting requirement[9]. Security must be considered as an inseparable part together with the development of network, but not as mechanisms added after-thought. Moreover, security can not be considered from a separate layer view. Today we have a lot of security mechanisms which work in different layer based on the OSI reference model's view: there is frequency hopping technique working in physical layer, WEP, 802.11x protecting data in data link layer, IPsec in network layer, and SSL/TLS, SSH in upper transport layer, and many application layer security protocols like Secure Electronic Transactions(SET), Privacy Enhanced Mail(PEM), etc. All of these security protocols are designed for specific security requirements and their overlapping functionalities make the whole system inefficient and complex and make it a big headache for users to choose and deploy.

Although some work has been done to increase the security of MANETs, none of them considers designing security mechanisms from a system architectural view. The lack of methodology to manage the complexity of security requirements in variant situations will lead to misplacement of security mechanisms and overlapping of security functionalities. The relevant work done so far either concerns with establishing the trust infrastructure alone, or just concerns with securing routing protocol based on certain assumptions that security associations are already established. The success of OSI model applied in designing network protocols is a good example for us to follow in designing security protocols. A layered architecture can provide

such advantages as modularity, simplicity, flexibility, and standardization of protocols. Follow this thought, we present here a layered secure architecture for MANETs in Figure 1. The figure depicts a five-layer security architecture for MANETs, and the functionalities of each layer are illustrated as below:

SL <sub>5</sub>	End-to-End Security
SL <sub>4</sub>	Network Security
SL <sub>3</sub>	Routing Security
SL <sub>2</sub>	Communications Security
SL <sub>1</sub>	Trust Infrastructure

**Figure 1. Security Architecture for MANETs**

1. SL<sub>1</sub>, Trust Infrastructure Layer: refers to the basic trust relationship between nodes, for example, like a well deployed PKI environment. Since in MANETs, there is no centralized authority to help establish the trust relationship between communicating nodes, the security mechanisms in this layer are expected to be constructed in a distributed manner and are the basic building block of the whole security system. Thus, SL<sub>1</sub> poses a great challenge to system security designers. The security association established in trust infrastructure layer must serve for the upper layer security mechanisms.
2. SL<sub>2</sub>, Communications Security Layer: refers to the security mechanisms applied in transmitting data frames in a node-to-node manner, such as security protocol WEP working in data link layer in OSI model, or physical protection mechanisms like frequency hopping Security Mechanisms deployed in this layer may keep data frame from eavesdropping, interception, alteration, or dropping from unauthorized party along the route from the source to the destination.
3. SL<sub>3</sub>, Routing Security Layer: refers to security mechanisms applied to routing protocols. In MANET, nodes exchange information about their knowledge of neighborhood connectivity and construct a view of the network topology so that they can route the data packets to the correct destinations. Every node is required to participate in the routing activity and routing is an important part to keep the network connected. Hence, SL<sub>3</sub> is of particular significance in MANETs. In fact, the routing security layer involves two aspects: secure routing and secure data forwarding. In secure routing aspect, nodes are required to cooperate to share correct routing information to keep the network connected efficiently; in secure data forwarding aspect, data packets on the fly should be protected from tampering, dropping, and altering by any unauthorized party.
4. SL<sub>4</sub>, Network Security Layer: refers to the security mechanisms used by the network protocols which performs sub-network access operations from end system to end system. For example, we can achieve the security services like peer entity authentication, confidentiality and integrity as the network layer security protocol IPsec provides, another example is the SMT mechanism from [10].
5. SL<sub>5</sub>, End-to-End Security Layer: refers to end system security, such as SSL, SSH, and any application-specific security protocol. The security protocols in this layer is independent of the underlying networking technology since the related security mechanisms are restricted to only intended parties. The provision of any security service in this layer is highly

dependent upon security requirements related to specific applications .

The motivation of dividing the security architecture into such five layers is rather straightforward. SL<sub>5</sub> defines the security mechanisms related to end application system, like SET, thus it is necessary to differentiate this layer from the underlying layers. SL<sub>4</sub> deals with network access control and network layer data packet protection. SL<sub>4</sub> is in fact the security layer working at the end of network fabric. The mechanisms deployed in this layer tackle the network security problems that can not be solved satisfactorily in the underlying routing protocols. SMT[10] working at SL<sub>4</sub> is a good example of security efforts done in the end systems as a remedy for the unreliable routing protocol. The reason we include the routing protocol security, i.e., SL<sub>3</sub> in the architecture is that the inherent cooperative nature in MANETs requires every node in the network acts both as a host which needs other nodes relaying information for it and also as a router to provide routing and relaying functions to other nodes. The security mechanisms in SL<sub>3</sub> are highly related to the network topology and are always designed with respect to specific routing protocol in use. SL<sub>2</sub> is a layer providing hop-to-hop communications security, i.e., it is related to the data link security and physical layer security in the wireless communications channel. We require a trust infrastructure in SL<sub>1</sub> be established before communication begin to function securely, an example is the trust infrastructure established using distributed threshold cryptography in [5][8].

The intrusion prevention mechanisms like encryption and signature do not eliminate the need for intrusion/misbehavior detection and response. Although the intrusion/misbehavior detection and response mechanisms are not distinctively specified in the system architecture, they are actually very important in MANETs security system and can be deployed in any layer of the system architecture according to the security requirements in each layer.

## 4. SECURITY ARCHITECTURE OF MILITARY APPLICATIONS

For mission-critical applications such as a military application in a hostile environment there are more stringent security requirements than in a MANET for commercial or personal uses. A military scenario may have higher requirements regarding both information security and routing topology security. In such a scenario, we may design the functionalities of each layer in security architecture as follows:

1. Data information is protected in a most fine-granular way in application layer, so the best way to protect data information according to their different requirement is at SL<sub>5</sub>. For example, it is highly desirable to handle data confidentiality and integrity in SL<sub>5</sub> layer, since this is the easiest way to protect data from altering, fabrication and compromise. This is especially important in a military scenario where strategic and tactical information is sent.
2. Since it is impossible to deploy a centralized firewall or security gateway in an ad hoc network, there is no way for any centralized security gateway to provide network access control services for mobile nodes. Thus the task of network access control and IP data packet protection lies on the end nodes. As IPsec protocol is not applicable to a mobile scenario, we need to exploit other means to protect data packet in SL<sub>4</sub>. For example, when the underlying routing protocol supports multi-

path routing, mechanisms from [15][10][11] working at  $SL_4$  can be used to take advantage of multi-route between the communicating routes to achieve higher reliability and increased data confidentiality when data packets are transmitted along the route from source to destination.

3. Military applications require to keep network topology secret and allow no traffic analysis in  $SL_3$ . Routing protocol designers should strive to hide the network topology from unauthorized party and should be designed carefully to prevent routing level attacks, like false routing updates, DoS attacks at routing protocols, thus security services such as confidentiality and integrity are expected to be provided in  $SL_3$ .
4. It is desirable to conceal communications in military scenario, and this requirement is most effectively fulfilled in  $SL_2$ . For example, we can take spread spectrum technologies to make the signal capture difficult or use antennas to influence signal power in space; and we can also deploy WEP or 802.1x to control the link access.
5. It seems quite natural to expect a PKI based on centralized or hierarchical offline CA to pre-establish the trust relationship for all the nodes due to the similar hierarchical relationships between soldiers and general, this is in fact infeasible due to the reasons that this can not handle the situation of compromise since CRL is difficult to deploy in a distributed environment in a timely manner. There is one trust model particularly suited for military scenario: Resurrecting Duckling Security Model [3], where a secure transient association is handled in a master-slave way which is like the hierarchical relationship between soldiers and their general. The security lies in the sense that master and slaves share a common secret, while the security association is only controlled by the master.

Compared with military applications, there may be relatively loose security requirements in commercial or personal scenarios, like security in routing protocol, confidentiality of network topology, and the basic trust infrastructure like PGP-like model[12] or maybe just location-limited-channel model[2] can be applied in these scenarios.

## 5. CONCLUSIONS

In this work we have dealt with security issues in mobile ad hoc networks. We have focused on designing a security architecture in tackling security challenges mobile ad hoc networks are facing. We present a security architecture in a layered view and analyze the reasoning for such a security architecture, and apply the proposed security architecture in military scenarios. we expect this security architecture can be used as a framework when designing system security for ad hoc networks.

## 6. ACKNOWLEDGEMENTS

We would like to thank Bell Labs Research China for supporting this research work.

## 7. REFERENCES

- [1] B. Dahill, B. Levine, E. Royer, and C. Shields. A Secure Routing Protocol for Ad Hoc Networks. Technical Report UM-CS-2001-037, CS Dept., UMass 2001.
- [2] D. Balfanz, D.K.Smetters, P.Stewart and H. Chi Wong: Talking To Strangers: Authentication in Ad Hoc Wireless Networks, appeared in Network and Distributed System Security Symposium, 2002.
- [3] F. Stajano and R. Anderson: The Resurrecting Duckling: Security Issues for Ad-Hoc Wireless networks. In Proceedings of the 7<sup>th</sup> International Workshop on Security Protocols, 1999.
- [4] H. Yang, X. Meng and S. Lu: Self-Organized Network-Layer Security in Mobile Ad Hoc Networks, ACM, 2002.
- [5] J. Kong, P. Zerfos, H. Luo, S. Lu, and L. Zhang, "Providing Robust and Ubiquitous Security Support for Mobile Ad Hoc Networks", Proc. Ninth Int'l Conf. Network Protocols(ICNP), Nov. 2001.
- [6]J-P. Hubaux, L. Buttyan and S. Capkun: The Quest for Security in Mobile Ad Hoc Networks, Proceedings of the 2<sup>nd</sup> ACM MobiHOC, 2001.
- [7] L.Buttyan, J. Hubaux Enforcing Service Availability in Mobile Ad-Hoc WANS, 1<sup>st</sup> IEEE/ACM workshop on Mobile Ad Hoc Networking and Computing, 2000.
- [8] L. Zhou and Z. Hass, "Securing Ad Hoc Networks" , IEEE network, vol 13, no.6 pp24-30, 1999.
- [9] P. Papadimitratos, Z. Haas, Secure routing for Mobile Ad Hoc Networks, Proceedings of CNDS , 2002.
- [10] P. Papadimitratos, Z. Haas, Secure Data Transmission in Mobile Ad Hoc Networks, ACM Workshop on Wireless Security, 2003.
- [11] S. Bonum, J.Ben-Othman, Data Security in Ad Hoc Networks Using MultiPath Routing, Proc. 14<sup>th</sup> IEEE International Symposium on Personal, Indoor and Mobile Radio Communication, 2003.
- [12] S. Capkun, L. Buttyan, J. Hubaux: Self-Organized Public-Key Management for Mobile Ad Hoc Networks, IEEE Transactions on Mobile Computing, VOL.1, NO.1, 2002.
- [13] S. Marti, T. Giuli, K.Lai and M.Baker: Mitigating Routing Misbehavior in Mobile Ad Hoc Networks, the 6<sup>th</sup> MobiCom 2000.
- [14] T. Gross, J.-P. Hubaux, J.-Y. Le Boudec and M. Vetterli: Toward Self-Organized Mobile Ad Hoc Networks: The Terminode Project", IEEE Communication Magazine, vol.39, issue 1, pp. 118-124, 2001.
- [15] W. Lou, W. Liu, Y. Fang: SPREAD: Enhancing Data Confidentiality in Mobile Ad Hoc Networks, IEEE INFOCOM, 2004.
- [16] Y. Hu, D.Johnson, A. Perrig: SEAD: Secure Efficient Distance Vector Routing for Mobile Wireless Ad Hoc Networks, Proc. IEEE workshop on Mobile Computing Systems and Applications, 2002.
- [17] Y. Zhang, W. Lee: Intrusion Detection in Wireless Ad-Hoc Networks, Proceedings of the 6<sup>th</sup> MOBICOM 2000 .