Sindh Univ. Res. Jour. (Sci. Ser.) Vol.44 (4) 609-612 (2012)

SINDH UNIVERSITY RESEARCH JOURNAL (SCIENCE SERIES)

On the Security Vulnerabilities in Mobile Adhoc Networks

E. SABA, I.A. QURESHI*, S. F. SHAH**, M. H. DEPAR, A. LATIF***

Information Technology Centre, SALU Tando Jam Pakistan

Received 29th August 2012 and Revised 13th October 2012

Abstract: In recent years mobile adhoc networks (MANETs) have been a very active research area mainly because of the typical nature of this environment and new challenges emerging thereof. The recent popularity of wireless devices is the driving force behind the research activities in this area. In addition to several other issues, security is one major challenge requiring appropriate solutions for this environment. There has been extensive research on the security issues in wired network environments, but those solutions are difficult to implement in the wireless environment and even more difficult in the wireless mobile adhoc environment. Some of the reasons include lack of central infrastructure and reliance on the participating users for relaying and routing of the messages, mobility of the nodes causing frequent changes in the network layout and limited memory, computational and battery power.

Keywords: MANET, infrastructure less wireless network, self configurable.

1. INTRODUCTION

A mobile adhoc network is a self configurable autonomous and infrastructure less wireless network. Users or nodes in the network can be moving or static; some nodes could be joining the network while others are leaving; some nodes may have very limited resources as compared to others and so on (Hubaux *et al.,* 2001).Thus it has a dynamic structure containing variable node status like the number of nodes in the network and active or passive nodes. Since the network is infrastructureless that is the network can be promptly deployed without relying on any existing infrastructure such as base station for wireless cellular networks , it requires cooperation of the participating nodes to carry out network operations. Such operations include forwarding and routing of the packets from other nodes, sharing network information and authorizing new nodes in the network.

The primary applications of mobile adhoc networks include military operations and disaster recovery operations where the environments are hostile and the operations are security sensitive requiring fast and reliable deployment (Cheng *et al.,* 2004).However due to the increasing popularity of wireless devices, the interest in mobile adhoc networks had been extended to everyday life such as on the fly setups for conferencing, mobile internet, academic institutions etc.

In the mobile adhoc network research area, most of the work has been focused on the development of network architecture, particularly on network routing protocols and MAC protocol design ,whereas relatively less work has been done on the security aspects. It is a proven fact now that if a given network architecture is not designed initially with proper security mechanisms, the security vulnerabilities will be exploited by malicious users and the network might be paralyzed by various types of attacks. Moreover addressing security issues as an afterthought can be expensive and inefficient (Buttyan *et al.,* 2000).Thus incorporating security issues in the networking architecture is a very important requirement for developing solutions for mobile adhoc networks.

2. MATERIAL AND METHODS

Security Vulnerabilities In Manets:

In the context of wired networks, security has been extensively studied and different applicable solutions are already in use. However due to the salient features (e.g infrastructureless, self organizing ,wireless channels ,mobility and limited resources)of mobiles adhoc networks , most of the security solutions for wired networks may not be applicable in this environment. Many new challenges (Yi *et al.,* 2001) associated with this environment include:

1. Wireless channels suffer from poor protection and are more vulnerable to different forms of attacks such as signal interference , eavesdropping and jamming.
2. Adhoc network routing protocols are cooperative in nature and depend on a trust relationship between nodes to route packets. This cooperative nature makes it much easier for impersonation, data tampering and denial of service (DoS) attacks.
3. The lack of a fixed infrastructure makes some conventional security mechanisms difficult to apply.
4. Mobile devices usually have limited bandwidth, slow processing, low battery power as well as limited radio transmission, all of which limit the practical deployment of comprehensive security schemes in mobile adhoc environments.
5. Continual and unpredictable mobility in adhoc networks makes the detection of normal and malicious behavior difficult.

++Corresponding author: I. A. QURESHI, i.ali1225@yahoo.com

*Department Of Telecommunication Engineering Mehran University Of Engineering And Technology Jamshoro Sindh Pakistan

*Information Technology Centre Sind Agriculture University Tando Jam Pakistan

3. RESULTS AND DISCUSSION

3.1 Defending against the physical attacks:

As mobile devices are small, light and easy to carry they are susceptible to loss and theft. In a battle field scenario they are at the risk of being hijacked or captured. Thus it is necessary to protect the physical security of the mobile devices. The conventional solution to the physical attack is to implement a security module like smart card that is tamper resistant.

3.2 Enforcing confidentiality:

Since the wireless channels in mobile adhoc networks is broadcast in nature , it suffers from poor protection and is particularly vulnerable to passive eavesdropping attacks. Confidentiality in this environment may consist of two aspects; one is to protect the identity of nodes and the other is to protect the transmitted messages from disclosure. In considering the first aspect , methods like hiding the nodes' transmission using spread spectrum technologies could be used whereas traffic analysis could be avoided using end to end encryption and link encryption. For the second aspect methods to secure the communication path could be avoided using encryption techniques and multipath routing (Haas *et al.,* 2002).

3.3 Authentication:

Authentication in an adhoc network could be achieved if a node shares a secret with another node then it can issue a challenge message (Dahill *et al.,* 2002) and request the correct answer. Upon receiving the correct answer , the other node is trusted to be the one sharing the secret .If both parties donot share a secret, a trusted third party (Certification authority CA) can be used for the verification with the understanding that both parties share secrets with the CA. Then the challenge process will be carried out between both parties through the CA. However in MANETs such centralized service is not possible therefore several distributed nodes have been deployed like distributed public key trust model (Broch *et al.,* 2003) where a selected set of nodes is used as servers or CAs that collaboratively manage the public keys. Another solution suggests a public key infrastructure based on a chain of trust instead of preselecting a set of nodes as the CAs as in (Michiardi *et al.,* 2002).

3.4 Key Management:

Key management is one of the most critical and complicated issues in the security of mobile adhoc networks, because the applicability of many other services such as authentication and confidentiality relies on efficient key management (Cheng *et al.,* 2004).

One approach to providing public key management service in wired or wireless cellular networks is the deployment of a public key infrastructure (PKI).The effectiveness of PKI depends on the security of a certification authority but the problem in applying in a mobile adhoc network is that such a central point is not practicable and even if it is deployed, it cannot be well protected and would become the most vulnerable point in the system. There are two methods to solve this problem. Firstly to retain the concept of certificate authority (CA), but distribute its functionality into multiple servers or trusted nodes .The other approach is to abandon the centralized Certificate authority and create a completely distributed and self organized key management system.

3.5 Handling Node Misbehavior:

In a mobile adhoc network, all basic functionalities such as routing and packet forwarding are collaboratively carried out by the participating nodes. The effectiveness of the network relies heavily on mutual trust and collaboration in sharing network resources. It is expected that all participants follow the rules according to the network design objectives. However there might exist some selfish nodes that do not want to provide services to other nodes so as to save their own battery power or to grasp more bandwidth, resulting in significant network performance degradation.

3.6 Intrusion Detection:

Intrusion detection relies on the assumption that the behavior of the intruder differs from that of a legitimate user. There are usually two approaches for detecting an intrusion; misuse or rule based detection and statistically anomaly detection.

3.7 Attacks on Routing protocols

Attacks on the routing protocols can be divided into two classes: active attacks and passive attacks Passive attacks include eavesdropping and traffic analysis. They are mainly a threat to the message confidentiality and do not affect the proper functioning of the routing protocols. Passive attacks on routing protocols can be avoided by protecting the data traffic. Active attacks can be further divided into internal and external attacks. External attacks are from outsiders and such attacks are limited when encryption and source authentication are utilized. Internal attacks, due to internal nodes are more severe because an internal node has all the necessary credentials for authentication. Some major attacks are classified as modification of routing information, fabrication of routing information, replay attacks and DoS attacks.

The protection of routing protocols can be achieved by implementing some kind of authentication and integrity schemes in the routing protocols so that the correctness of the routing information, particularly the node integrity, the destination sequence number and cost metric can be protected. Following are the methods incorporated with different proposed protocols.

Table 1: Various attacks on routing protocols pertinent to MANETs

S. No	Attacks	AODV[1]	SAODV[2]	ARAN[3]	DSR[4]	SRP[5]	DSDV[6]	SEAD[7]	Ariadne[8]
1	Impersonation	√	†	†	†	†	√	√	†
2	Spoofing	√	†	†	†	†	√	†	√
3	Replays	†	†	†	√	†	†	√	†
4	Fabrication of error messages	√	†	√	†	†	√	√	√
5	Fabrication of source routes (route cache poisoning)	†	†	†	†	√	√	†	†
6	Wormhole attack	√	√	√	√	√	†	√	†

√ Vulnerable † Protected (Results are based on studies and may vary in different

[1]AODV-Adhoc on demand distance vector routing
[2]SAODV –Secure Ad hoc on demand distance vector routing Zapata *et al 2002*
[3]ARAN-Authenticated routing for adhoc networks(Dahill *et al* 2002)
[4]DSR-Dynamic source routing
[5]SRP- Secure routing protocol(Papadimitratos *et al* 2002)
[6]DSDV-Destination sequenced distance vector(Perkins *et al*, 2004)
[7]SEAD-Secure efficient adhoc distance vector routing (Hu *et al* , 2002)
[8]Ariadne-(ChunHu *et al*, 2002)

4. Securing Routing Protocols:

The current routing protocols for adhoc networks are not designed to accommodate defense against malicious attackers and are therefore highly vulnerable to attacks. There are two broader levels of attacks pertinent to adhoc networks.

4.1 Attacks on the Basic mechanism:

Attacks on the basic mechanism constitute of routing and packet forwarding attacks. It is categorized as attacks based on modification and based on fabrication of information. The former attack is the simplest yet most effective way to disturb the operations of an adhoc network by a malicious node. Here the malicious node just broadcasts better routes than the ones presently existing. It includes redirection by changing the route sequence number, redirection by altering the hop count, Denial of service by altering routing information. The later attack based on fabrication of information is a set of attacks so as to fabricate or modify the information .This includes route cache poisoning, falsification of route error messages and routing table overflow attack.

4.2 Attacks on the Security mechanism:

Attacks on the security mechanism constitute of key management and authentication .In almost any network the basic security mechanism requires that the user makes use of the appropriate cryptographic keys. This is hard to achieve in adhoc network where the different nodes move around. A few typical scenarios of such attacks may include malicious replacement of public keys, and if there is a distributed trust authority it can be overwhelmed by malicious node.

4.3 Protecting the Basic mechanism:

Two most commonly used approaches are Prevention techniques and Detection and reaction techniques. In prevention technique the malicious nodes are prevented from initiating attacks. It achieves this task by employing encryption techniques to provide authentication, integrity, confidentiality and non repudiation of routing information. In the existing preventive approaches some techniques either use asymmetric algorithms/symmetric algorithms or one way hashing . SAODV and ARAN are routing protocols employing prevention using asymmetric cryptography. SAR and SRP use prevention using symmetric cryptography whereas SEAD and Ariadne utilize prevention using one way hash chains.

Table 2: Requirements of various routing protocols pertinent to MANETs

S No	Requirements/Issue	AODV	SAODV	ARAN	DSR	SRP	DSDV	SEAD*
1	Authentication	Vulnerable	End to end	Point to point	Not addressed	End to end	Not addressed	Point to point
2	TA/CA†	Not required	Not required	Required	Not required	Not required	Not required	Required
3	Key revocation	Not addressed	Not addressed	Broadcast	Not addressed	Not addressed	Not addressed	Not addressed
4	Integrity	Compromised	Addressed	Vulnerable	Vulnerable	Addressed	Vulnerable	Addressed
5	Non repudiation	Compromised	Addressed	Vulnerable	Vulnerable	Addressed	Vulnerable	Addressed
6	Selfishness	Not addressed	Not addressed	Not addressed	Not addressed	Not addressed	Not addressed	Not addressed

*SEAD-Secure efficient distance vector (Hu *et al* 2002) †TA/CA-Trusted authority/Certification authority

Detection techniques on the other hand try to identify any malicious activity in the network and take corrective action against such nodes. Protocols like CONFIDANT (Buchegger *et al.,* 2002).

4.4 Protecting the Security Mechanism:

The most critical and complex issue in securing adhoc networks is key establishment which can be addressed by key agreement or key transport. In key agreement, a shared key is derived by two or more parties as function of information associated with each of these, in such a way that none of the parties can predetermine the resulting value. In key transport one party creates a secrete value and safely transfers it to the others. Both approaches can be based on symmetric or asymmetric techniques. Asymmetric key cryptography is more suitable for adhoc networks because it does not require online trusted servers however there is a demerit in the form of key revocation.

Table 3: Security issues in various security schemes used in MANETs

S No	Security Issues	PKCS[1]	Self organized PKI[2]	Threshold cryptography[3]	IBE[4]
1	Requirement of CA[5]	Fundamental	Required only for private key	Distributed among nodes	Required only for private key
2	Public key certification	Provided	Based on PGP	Distributed	Not required
3	Key expiration and revocation	Owner gets private key reissued, all others get the new public key certificate	Trust graph	Distributed	Not addressed
4	Contact with CA	Frequent	Less frequent	Not required	Less frequent
5	Certificate directory	Maintained	Local certificate repository	Not required	Not maintained
6	Memory consumption	Inherent	Certificate issued are saved	Not inherent	Not inherent
7	Public keys	Certified by CA	Merging of certificate repositories	Initially distributed	Bind to identities
8	Draw back	Public key certification, frequent contact with CA	Selfishness, complex algorithms required	Selfishness, complex algorithms required	Identity binding

[1]PKCS Public Key Cryptosystems (Capkun *et al.*, 2002)
[2]2Self organized PKI-Self organized Public key infrastructure (Capkun *et al* 2002)
[3]Threshold cryptography (Desmedt *et al* 2001)
[4]4IBE Identity Based Encryption(Boneh *et al* ., 2001, Shamir 1987)
[5]CA Certificate Authority

5. CONCLUSION

The existing Mobile Adhoc network security solutions pose daunting but exciting research challenges. It is an interesting challenge to build an efficient barrier that takes care of each device in the network. However due to the inherent lack of infrastructure in adhoc networks, security solutions for MANETs have to cope with difficult environment including scarce resources like energy and dynamic topology for security.

The solutions presented here only cover a few of all the threats and are unable to provide a comprehensive answer to all the security problems in adhoc networks. These solutions often address isolated issues but are far from a comprehensive solution to security in adhoc networks. As more and more research is carried on in the field of adhoc networks, comprehensive security solutions would surface that would be helpful in addressing all prevalent issues in adhoc networks including routing protocols, key management and cooperation enforcement.

REFERENCES:

Bucheggar, S. and J.Y.L. Boudec (2001)"The selfish node, increasing routing security in Mobile adhoc networks",IBM research report RR 3354.

Buttyan, L. and J.P. Hubaux, (2000) "Enforcing service availability in mobile adhoc networks". In the proceedings of the 1st ACM international symposium on Mobile Adhoc Networking and computing – MobiHoc'00, 87-96.

Boneh, D. and M. Franklin (2001)"The identity based encryption from the Weil Pairing", in the proceedings of the advances in cryptography, crypto'01, 229-231.

Capkun, S., L. Buttyan and J.P. Hubaux (2002)" Public key management for mobile adhoc networks", In ACM International workshop on wireless security.

Cheng, X., X. Huang and D.Z. Du, (2004) "Adhoc Wireless Networking ,Survey of Wireless security in Mobile Ad hoc Networks: challenges and available solutions", Kluwer academic publishers, 319-364.

ChunHu, Y., A. Perrig and D.B. Johnson (2002) Ariadne: A secure on demand routing protocol for adhoc networks Mobicom 2002, Atlanta Georgia USA.23-28.

Dahill, B., B. N. Levine,E.Royer and C. Shields (2002)"A secure routing protocol for Adhoc networks", In the proceedings of the 10th conference on Network protocols (ICNP).

Hubaux, J.P., L. Buttyan and S. Capkin, (2001) "The Quest for security in Mobile Adhoc Networks", In the proceedings of the 2nd ACM International Symposium on Mobile Adhoc Networking and Computing – MobiHoc'01.

Hu, Y.V., A. Perrig and D. B. Johnson (2002) "SEAD:secure efficient distance vector routing for mobile wireless adhoc networks". In the proceedings of the IEEE workshop on mobile computing systems and applications.

Michiardi, P.and R. Molva (2002)"Simulation analysis of security exposures in mobile adhoc networks", proceedings of European wireless conference.

Marti. S., T. Giuli, K. Lai and M. Baker (2000)"Mitigating routing misbehavior in mobile adhoc network," In the proceedings of the 6th annual ACM/IEEE International conference on mobile computing and networking Boston USA, 255-265.

Shamir. A. (1987) "Identitiy based cryptosystems and signature schemes". In the proceedings of advances in cryptography, crypto'84 Vol. **(196)**: pf lecture notes in computer science, Springer Verlog, 47-53.

Zapata, M.G. (2002) Secure Adhoc on demand distance vector (SAODV) Buchegger, S, J.Y.L. Boudec (2001)" Performance analysis of the CONFIDANT protocol". In proceedings of MobiHoc 2002.