Proceedings of the 4th National Conference; INDIACom-2010
Computing For Nation Development, February 25 – 26, 2010
Bharati Vidyapeeth's Institute of Computer Applications and Management, New Delhi

Performance Evaluation of Protocols for Secure Routing over MANET

Sunil Taneja
Government P.G. College, Kalka,
India suniltaneja.iitd@gmail.com

Ashwani Kush
University College,
K.U.K, India
akush20@gmail.com

Amandeep Makka
Arya Girls College,
Ambala Cantt, India
aman.aryacollege@gmail.com

ABSTRACT

A recent trend in Ad Hoc network routing is the reactive on-demand philosophy where routes are established only when required. Most of the protocols in this category are not incorporating proper security features. The ad hoc environment is accessible to both legitimate network users and malicious attackers. It has been observed that different protocols need different strategies for security. This paper provides an overview of various secured routing protocols by presenting their characteristics, functionality & security issues and then makes their comparative analysis so to analyze their performance. The objective is to make observations about how the performance of these protocols can be improved. Basically, attacks on ad hoc network routing protocols disrupt network performance and reliability. The objective of this paper is to highlight major security issues and then suggest appropriate solutions by analyzing existing protocols. An attempt has been made to standardize the approaches for security concerns.

KEY WORDS

MANET, Security, Secure Routing, Ad hoc networks.

1.0 INTRODUCTION

A Mobile Ad Hoc Network (MANET) is a collection of wireless mobile nodes forming a temporary/short-lived network without any fixed infrastructure where all nodes are free to move about arbitrarily and where all the nodes configure themselves. Unlike traditional networks whereby routing functions are performed by dedicated nodes or routers, in MANET, routing functions are carried out by all available nodes. There are no fixed base stations and each node acts both as a router and as a host. Even the topology of network may also change rapidly. The mobile nodes in the Ad Hoc network dynamically establish routing among themselves to form their own network 'on the fly'. In essence, the network is created in ad-hoc fashion by the participating nodes without any central administration.

Ad hoc networks are primarily meant for use by military forces or for emergency rescue situations. At the state of war an army cannot rely on fixed infrastructure, as it is an easy and attractive target for the enemy. Ad hoc networks are optimal solution in such cases. For civil use ad hoc networks are crucial if the fixed infrastructure has been torn down by some natural disaster, like a flood or an earthquake. Then rescue operations could in such a situation be managed through utilizing ad hoc networks. Implementing an ad hoc network is a challenging task and some of the challenges in its implementation include:

1. Unicast/ Multicast routing
2. Dynamic network topology
3. Speed/Mobility
4. Link stability
5. Frequency of updates or Network overhead
6. Scalability
7. Quality of Service
8. Energy efficient/Power aware routing
9. Secure routing

2.0 SECURITY ATTACKS ON ADHOC NETWORKS [5,7,12]

Since the security of the modern wireless networks does not seem to be so affirmative, there have been several proposals to solve security related issues but the problem is that they target specific threats separately. Therefore, there is a requirement to have an efficient security system which takes care of all aspects of security. Network security attacks are typically divided into two categories: passive vs. active attacks and external vs. internal attacks.

Passive vs. Active attacks [5,7]

A passive Attack is that attack in which an unauthorized party gains access to an asset and does not modify its content. The passive attacker does not send messages; it only eavesdrops on the network. The malicious entity in this type of attack only listens to the traffic, without modifying or disturbing it in any way. The main threat by such an attack is that some confidential information is leaked to the attacker. Passive attacks can be either eavesdropping or traffic analysis.

Eavesdropping: The attacker monitors transmissions for message content. An example of this attack is a person listening into the transmissions on a network topology between two workstations or tuning into transmissions between a wireless handset and a base station.

Traffic analysis/Traffic flow analysis: The attacker, in a more subtle way, gains intelligence by monitoring the transmissions for patterns of communication. A considerable amount of information is contained in the flow of messages between communicating parties.

An active attack is that attack in which an unauthorized party makes modifications to a message, data stream, or file. In an active attack, the malignant node actively disturbs the normal operation of the network. This can be done by forging packets, disrupting normal routing or consuming network resources etc. Active attacks may take the form of one of four types masquerading, replay, message modification, and denial-of-service (DoS). These attacks are summarized as:

Masquerading: The attacker impersonates an authorized user and thereby gains certain unauthorized privileges.

Replay: The attacker monitors transmissions (passive attack) and retransmits messages as the legitimate user.

Message modification: The attacker alters a legitimate message by deleting, adding to, changing, or reordering it.

Denial-of-service: The attacker prevents or prohibits the normal use or management of communications facilities.

External vs. Internal attacks [12]

External attacks, in which the attacker aims to cause congestion, propagate fake routing information or disturb nodes from providing services. Internal attacks, in which the adversary wants to gain the normal access to the network and participate the network activities, either by some malicious impersonation to get the access to the network as a new node, or by directly compromising a current node and using it as a basis to conduct its malicious behaviors. In the two categories shown above, external attacks are similar to the normal attacks in the traditional wired networks in that the adversary is in the proximity but not a trusted node in the network, therefore, this type of attack can be prevented and detected by the security methods such as membership authentication or firewall, which are relatively conventional security solutions. However, due to the pervasive communication nature and open network media in the mobile ad hoc network, internal attacks are far more dangerous than the external attacks: because the compromised nodes are originally the benign users of the ad hoc network, they can easily pass the authentication and get protection from the security mechanisms. As a result, the adversaries can make use of them to gain normal access to the services that should only be available to the authorized users in the network, and they can use the legal identity provided by the compromised nodes to conceal their malicious behaviors. Therefore, we should pay more attention to the internal attacks initiated by the malicious insiders when we consider the security issues in the mobile ad hoc networks.

3.0 EXISTING SOLUTIONS [1,2]

The consequences of these attacks include, but are not limited to, loss of proprietary information, legal and recovery costs, tarnished image, and loss of network service. Some of the measures that can be incorporated are:

1. **Virtual Private Networks (VPN)** This offers a solid solution to many security issues, where an authenticated key provides confidentiality and integrity for Internet Protocol data grams. Software are available to implement VPNs on just about every platform. Authentication depends upon three factors such as password, fingerprints and a security token.
2. **Encryption:** Encryption is a technique used for many years for passing information from one place to other in a secured manner. A message in its original shape is referred to as a plaintext (or Text) and a message used to conceal original message is called Ciphertext (or Cipher). The process of changing plaintext into ciphertext is called Encryption and the reverse process is called decryption. There are many algorithms available for these processes. Some of them are Data Encryption Standard (DES), International Data Encryption algorithm (IDEA) and Public key algorithm (RSA). These algorithms are key based algorithms.
3. **One Way Hash Function**: There is another algorithm called one way hash Function. It is like checksum of a block of text and is secure. It is impossible to generate the same hash function value without knowing the correct algorithm and key. It accepts a variable size message and produces an affixed size tag as output.
4. **Digital Signature**: A digital signature is an electronic signature that can be used to authenticate the identity of the sender or the signer of a message/document, and possibly to ensure that the original content of the message or document that has been sent is unchanged. Digital signatures are easily transportable, cannot be imitated by someone else, and can be automatically time-stamped. External attacks can be checked using Confidentiality of the routing information and also by authentication and integrity assurance features. Encryption can be solution to this. Digital signature can be applied.

4.0 COMPARATIVE STUDY AND PROPOSED SOLUTION

Based on the existing protocols, an effort has been made to chalk out strategy adopted by each protocol, its merits and demerits. Following is the Table 1 describing comparative study of security protocols. As is clear from comparative study of different protocol compiled in Table 1, there is no single solution for the problem of security. Another important point to emphasize is the different protocols will need different solutions. So selection of proper technique becomes critical. The proposed scheme is based on public key cryptography. The governing authority that creates the network is the only entity that has the *system private key*. Each node is given a public/private key pair by the authority. The system private key is used to sign the public keys of all the nodes. This signing of the public key takes place off-line before the node can join the network. This can be done securely by making use of traditional security schemes for wired networks or can be physically incorporated into the nodes. Each node is also given the *system public key*. Whenever two nodes interact for the first time, the certified public keys are exchanged. Since the nodes have the system public key, the authenticity of the certificate can be confirmed. Since only the governing authority has the system private key, it is secure. Moreover this authority is well protected since it is not mobile like the other nodes. The proposed solution is based on key cryptography for

AODV protocol as it is most widely accepted and used in ad hoc environments. It has been studied that the same technique can be applied to DSR as well.

Table 1: Summary of secure routing protocols

Name of the protocol	Features
[9] SRP	a) This assumes security association between source destination nodes. b) Intermediate nodes do not need cryptography. c) Adds a SRP header to base routing protocol. It has three parts taking care of old outdated requests, prevents fabrication and ensures integrity.
[3] ARAN	a) Assumes managed-open environment. b) First stage is certification and end-to-end authentication stage. Source takes a trusted certificate from trusted server, signs the request packet. Each intermediate node signs the request with its certificate. c) Computationally expensive.
[13] ARIADNE	a) Uses highly efficient symmetric key cryptography b) No guard against passive attackers. c) Does not prevent insertion of malicious data packets. d) Vulnerable to other attackers form broken link.
[14] SEAD	a) Uses one way hash function. b) Attacker cannot generate any value in hash chain. c) Very efficient mechanism.
[8] SAODV	a) Implementation on AODV. b) Checks external attacks. c) Uses Key cryptography and hashing both. d) High overhead.
[11] SAR	a) Classifies nodes into different immutable trust levels. b) Can be implemented by distributing keys for each trust level. c) Not very scalable. d) Lot of computational efforts required.

5.0 CONCLUSION

Analytical study has been carried out for existing security routing protocols for wireless mobile ad hoc networks. A summary of their key attributes is presented in Table 1. We have tried to identify areas where some further work needs to be done. The security problems assume monumental proportions especially in the case of ad hoc networks as there is no central governing authority. There is a need for a mechanism to salvage the routes in case of node failure. The proposed scheme is intended for AODV and efforts are on to check performance of the scheme via simulations.

6.0 FUTURE SCOPE

The future study will give further analysis of the scheme compared with other existing secured protocols. The research on MANET security is still in its early stage. The existing proposals are typically attack-oriented in that they first identify several security threats and then enhance the existing protocol or propose a new protocol to overcome such attacks. Because the solutions are designed explicitly with certain attack models in mind, they work well in the presence of designated attacks but may collapse under unanticipated attacks. Therefore, a more ambitious goal for ad hoc network security is to develop a multifold security solution, resulting in in-depth protection that offers multiple lines of defense against many both known and unknown security threats.

7.0 REFERENCES

[1] Ashwani Kush, “Security and Reputation Schemes in Ad-Hoc Networks Routing”, International Journal of Information Technology and Knowledge Management, Volume 2, No. 1, pp. 185-189, January June 2009.

[2] A. Kush “Security Aspects in AD hoc Routing”, Computer Society of India Communications, Vol. no 32 Issue 11, pp. 29-33, March 2009.

[3] Dahill, B. N. Levine, E. Royer and C. Shields, “A secure routing protocol for ad hoc networks”, Technical Report UM-CS-2001-037, University of Massachusetts, Department of Computer Science, Aug. 2001.

[4] C.K. Toh,, “Ad hoc mobile wireless Networks”, Prentice Hall, New Jersey, 2002.

[5] D. B. J., Yih-Chun Hu, Adrian Perrig, “Ariadne: A secure on-demand routing protocol for ad-hoc networks”, Proceedings of the Eighth Annual International Conference on Mobile Computing and Networking (MobiCom 2002), Sept. 2002.

[6] Dimitri Bertsekas, Robert Gallager, “Data Networks: 2nd Editions” Prentice Hall, New Jersey, ISBN 0-13-200916-1.

[7] Kai Inkinen, “New Secure Routing in Ad Hoc Networks: Study and Evaluation of Proposed Schemes”, Helsinki University of Technology T-110.551, Seminar on Internetworking, Sjökulla, 2004-04-26/27.

[8] L. Zhou and Z. J. Haas, “Securing ad hoc networks”, IEEE Network Magazine, 13(6):24–30, November/ December 1999.

[9] P. Papadimitratos and Z. J. Haas, “Secure routing for mobile ad hoc networks”, SCS Communication Networks and Distributed Systems Modeling and Simulation Conference (CNDS 2002), Jan 2002.

[10] Seung Yi, Prasad Naldurg, Robin Kravets, "Security-Aware Ad-hoc routing for wireless networks", Technical Report No. UIUCDCS-R-2001-2241, August 2001 and In Proceedings of the 2nd ACM international symposium on Mobile ad hoc networking & computing 2001, Long Beach, CA, USA, October 04 - 05, 2001.

[11] S. Yi, P. Naldurg, R. Kravets, "A security-aware ad hoc outing protocol for wireless networks", 6th World Multi-Conference on Systemics, Cybernetics and Informatics (SCI 2002), 2002.

[12] Wenjia Li, Anupam Joshi, "Security Issues in Mobile Ad Hoc Networks- A Survey", Department of Computer Science and Electrical Engineering, University of Maryland, Baltimore County, http://www.cs.umbc.edu/~wenjia1/ 699_report.pdf, 2008

[13] Y. C. Hu, A. Perrig and D. Johnson, "Ariadne: A secure on-demand routing protocol for ad hoc networks", Technical Report TR01-383, Rice University, Dec. 2001.

[14] Y.-C. Hu, D.B. Johnson, A. Perrig, 'SEAD: secure efficient distance vector routing for mobile wireless ad hoc networks", Proceedings of the 4th IEEE Workshop on Mobile Computing Systems & Applications (WMCSA 2002), pp. 3–13, IEEE, Calicoon, NY, June 2002.

Continued from Page No. 190

Digital signature ensures integrity, non-repudiation and euthenics of the cheque. To prevent forgery and alterations payer's digital signature is embedded into digital image of the cheque using robust watermarking technique [6]. Payer then issues the cheque to payee. The issue process generates a sequence number to give uniqueness to each cheque. To achieve confidentiality, the cheque image can be encrypted using RSA algorithm using payee's public key.

B. Payee End

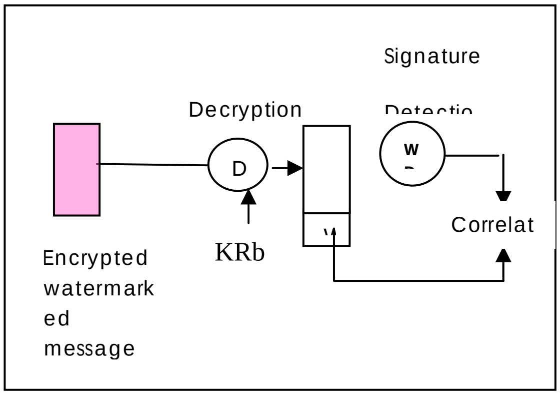

Figure 2 : Authenticity checking process

After receiving the digital cheque, payee decrypts the cheque image using his private key. Payee verifies payer's digital signature using correlation technique to test authenticity of the legitimate account holder [11, 12]. Then payee further signs the cheque with his digital signature to endorse it to the presenting bank for further fund settlement.

Once the image is available to the presenting bank, it can follow conventional CTS for clearance with IDRBT standards and appropriate Indian Acts.

7.0 EXPERIMENTAL RESULTS

We conducted an experiment to embed digital signature in structured electronic document like e-cheque to transfer funds from payer's account to payee's account. We used a 32-bit RGB model to represent the cheque image using JAVA advanced imaging classes. We used SHA-1 algorithm to find message digest and RSA algorithm to encrypt message digest. We orthogonalized signature With respect to average vector found from selected block We embedded a scale version of orthogonalized signature back to the selected block. PSNR is set to minimum 30 DB to avoid white noise. Overall image is encrypted with public key of the recipient to achieve confidentiality and integrity. Signature is detected using correlation analysis, figure 6 shows that correlation factor corresponding to true signature is between 0.9 and correlation factor corresponding to false signature is negative or below 0.6.

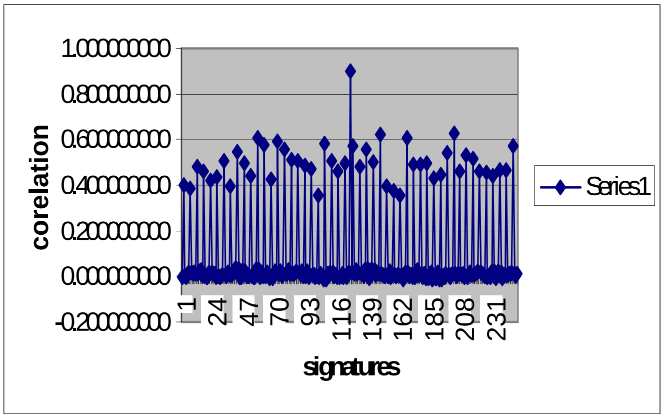

Figure 3 : Correlation spread of watermarked image. Central spike corresponds to true signature and other points to randomly generated candidate signature

8.0 CONCLUSION

Cheque payment system is vulnerable to frauds due to manual verification of cheque data on paper cheque. Indian banking industry experienced many forgery and alteration cases in cheque before it is presented for clearing. For technical excellence and business value of cheque payment system, security of information plays an essential role. Cryptography alone can be an effective solution to all these problems but in most of instances in the form of costly and specialized hardware to create tamper proof devices.

Continued on Page No. 198

Continued from Page No. 190

In this paper we have presented a software-based approach, which combines digital signature technology with robust watermarking technique to achieve authenticity, confidentiality, integrity and restricting alteration and forgery in information. The proposed technique is tested to prevent forgery of signature and alteration of information in cheques.

9.0 FUTURE SCOPE

The suggested scheme can be directly plugged into present cheque truncation system in Indian perspective to prevent forgery and alterations in cheques. Moreover, the designed application can only be implemented fully, if each end-user is being provided digital certificate so that server can authenticate the user by PKI instead of username and password.

10.0 REFERENCES

[1] RBI department of payment & settlement," Review of Payment & Settlement Systems. in India. 2006 – 2007", April 2007, pp 03-07.

[2] Staff Reporter, "Bank staffer among three arrested for cheating," THE HINDU, para. 3, July 29,2004. [Online].Available:http://www.hindu.com/2004/07/29/stories/2004072915260300.htm [Accessed on July, 15, 2009]

[3] Staff Reporter, "Two held on forgery charge," *THE HINDU*, para. 3, April 06, 2007. [Online]. Available: http://www.thehindu.com/2007/04/06/stories/2007040612820500.htm, [Accessed on May 10, 2008]

[4] Aiswarya. A, "3 Held for attempted forgery of cheque," expressindia, para. 3, Jan 13, 2009. [Online]. Available: http://www.expressindia.com/latest-news/3-held-for-attempted-forgery-of-cheque/410087/ [last accessed on 19-aug-2009]

[5] Staff Reporter, "Cheque fraud case: Andhra Bank deputy manager held," *THE HINDU*, para. 3, July 02, 2009. [Online]. Available: http://www.thehindu.com/2009/07/02/stories/2009070260600500.htm [Accessed Aug. 18, 2009].

[6] RBI department of payment & settlement, "FAQ on CTS in national capital region"

[7] Milton M. Anderson , "The Electronic Check Architecture (FSTC)", September 29, 1998., Version 1.0.2,pp01-07.

[8] National Institute of Standards and Technology, Fips 180, Federal Information Processing Standards, Secure Hash Standard (SHS), April 1993.

[9] D.Eastlake .3rd, P.Jones.US , " Secure Hash Algorithm-1(SHA-1), September,2001.

[10] Balas Natrajan, " Robust Public-Key Watermarking of Digital Images", Computer Systems Laboratory, HPL,97-118, October, 1997.

[11] B.P.Lathi, " Modern Digital and Analog communication system",Oxford University Press , third edition, 1998, pp 406-416.

[12] Rafael.C Gonzalez, Richard. E.Woods , " Digital image processing "Person education, seventh edition(2001), pp111.