Secured Scheme for Ad hoc Networks using Encryption as a Tool

Sima	**Shayog Sharma**	**Viney Dhawan**	**Mandeep Kaur**
Department of CSE	*Research Scholar in CSE*	*Department of ECE*	Research Scholar *in CSE*
KITM Karnal,	NCCE Isarana	KITM Karnal	DVIET Karnal
Haryana, India	Haryana, India	Haryana, India	Haryana, India

Abstract*— *Ad hoc networks are a new wireless networking paradigm for mobile hosts. Unlike traditional mobile wireless networks, ad hoc networks do not rely on any fixed infrastructure. Routing in ad-hoc networks is nontrivial due to highly dynamic environment. In recent years several routing protocols targeted at mobile ad-hoc networks are being proposed and prominent among them are DSDV, AODV, TORA, and DSR. It has been observed that different protocols need different strategies for security. The cryptic algorithm has been proposed in this paper. This scheme can make most of the on-demand routing protocols secure. The study will help in making protocols more robust against attacks and standardize parameters for security in protocols.

Keywords*— *Security, Ad hoc Networks, Routing Protocols, Key Management

I. INTRODUCTION

In an ad hoc network, without a fixed infrastructure nodes can communicate. Node mobility in an ad hoc network causes frequent changes of the network topology. The nodes themselves are responsible for routing the packets. The nodes in an ad-hoc network can be a laptop, PDA, or any other device capable of transmitting and receiving information. Network is temporary as nodes are generally mobile and may go out of range of other nodes in the network. If routing is misdirected, the entire network can be paralyzed. The problem is enlarged by the fact that routing usually needs to rely on the trustworthiness of all the nodes that are participating in the routing process. It is hard to distinguish compromised nodes from nodes that are suffering from bad links. In this paper, the ad hoc networks trust evaluation based security solution has been analyzed. The main goal of the security solutions for an Ad Hoc network is to provide security services, such as authentication, confidentiality, integrity, anonymity and availability to mobile users [1]. In an ad hoc wireless network where wired infrastructures are not feasible, energy and bandwidth conversation are the two key elements presenting research challenges. limited bandwidth makes a network easily congested by control signals of the routing protocol. Routing schemes developed for wired networks seldom consider restrictions of this type. Instead, they assume that the network is mostly stable and the overhead for routing messages is negligible. Considering these differences between wired and wireless network, it is necessary to develop a wireless routing protocol that restricts congestion in the network [22][23][24][21][12][13]. The rest of the paper is organized as follows. Section two discusses the security problems in the ad hoc networks. Section three presents the current security schemes in the literature. In section four, a trust evaluation based solution for the ad hoc networks is proposed. In the next section, the solution is illustrated by a routing protocol and proved by analyzing its security against several active attacks Finally, the conclusions and directions of future work are given in the last section. Since an ad hoc network can be deployed rapidly with relatively low cost, it becomes an attractive option for commercial uses such as sensor networks or virtual classrooms.

.

II. ATTACK ON AD HOC NETWORK

An The salient characteristics of the ad hoc networks pose challenges to security [11-13]. **First** of all, the use of wireless link renders an ad hoc network susceptible to link attacks. These attacks can be broadly classified into two main categories as: Passive attacks and Active attacks.

- **Passive Attacks**

Passive attacks are the attacks in which an attacker does not actively participate in bringing the network down. The nature of attacks varies greatly from one set of circumstances to another. Some of the generic types of attack [2,3,4,5,6,8,9] that might be encountered in passive attacks.

- **Active Attacks**

These attacks involve some modification of the data stream or the creation of a false stream. Various types of attacks on ad hoc network which are describing following:

- **Location Disclosure:** Location disclosure is an attack that targets the privacy requirements of an ad hoc network. Through the use of traffic analysis techniques [7], or with simpler probing and monitoring approaches, an attacker is able to discover the location of a node, or even the structure of the entire network.
- **Black Hole:** In a black hole attack a malicious node provides false route replies to the route requests it receives, advertising itself as having the shortest path to a destination[16]. These fake replies can divert network traffic via malicious node for eavesdropping, or simply to attract all traffic in order to perform a denial of service attack by dropping the received packets.
- **Interruption:** An asset of the system is destroyed, becomes unavailable or unusable. This is an attack on availability. Examples include destruction of a piece of hardware, or cutting of a communication line.

- **Interception:** An unauthorized party gains access to an asset. This is an attack on confidentiality. The unauthorized party could be a person, a program or a computer. Examples include wiretapping to capture data in a network or the illicit copying of files.
- **Modification:** An unauthorized party tampers with an asset. This is an attack on integrity. Examples include changing values in a data file or modifying the contents of a message being transmitted in a network.
- **Fabrication:** An unauthorized party inserts malicious objects into the system. This is an attack on authentication. Examples include the insertion of spurious messages in a network or the addition of records to a file.
- **Replay:** This involves capture of data units and its subsequent retransmission to produce an unauthorized effect. Sniffers are used for legitimate network management functions.
- **Wormhole:** The wormhole attack is one of the most powerful presented here since it involves the cooperation between two malicious nodes that participate in the network [17].
- **Blackmail:** This attack is relevant against routing protocols that use mechanisms for the identification of malicious nodes and propagate messages that try to blacklist the offender [18].
- **Replacement:** In this attack one entity pretends to be a different entity. This is a type of attack that is used by someone familiar with your security procedures and failures.
- **Denial of Service:** This prevents the normal use or management of communication facilities. One form of service denial is the disruption of an entire network, either by disabling the network or by overloading it with messages so as to degrade the performance. Denial of service attacks aim at the complete disruption of the routing function and therefore the entire operation of the ad hoc network [19].
- **Rushing Attack:** Rushing attack is that results in denial-of-service when used against all previous on-demand ad hoc network routing protocols [20]. For example, DSR, AODV, and secure protocols based on them, such as Ariadne, ARAN, and SAODV, are unable to discover routes longer than two hops when subject to this attack.
- **Modification of Messages:** This simply means that some portion of a legitimate message is altered, delayed or reordered. Here someone between you and your connection works as an intermediary, listening in on your communications and possibly modifying them.

It seems difficult to provide a general security solution for the ad hoc networks. Traditional cryptographic solution is not adapted for the new paradigm of the networks. As can be seen from the above analysis, what is lacked in the ad hoc networks is trust since each node must not trust any other node immediately. If the trust relationship among the network nodes is available for every node, it will be much easier to select proper security measure to establish the required protection. It will be wiser to avoid the un-trusted nodes as routers. Moreover, it will be more sensible to reject or ignore hostile service requests. Therefore, the trust evaluation becomes a before-security issue in the ad hoc networks. The security solution should be dynamic based on the changed trust relationship.

III. Key management

Traditional cryptographic mechanisms, such as digital signature and public key encryption, still play vital roles for the security of the ad hoc networks. All these mechanisms require a key management service to keep track of key and node binding and assist the establishment of mutual authentication between communication nodes. Traditionally, the key management service is based on a trusted entity called a certificate authority (CA) to issue public key certificate of every node. The trusted CA is required to be online in many cases to support public key revocation and renewal. But it is dangerous to set up a key management service using a single CA in an ad hoc network. It will be the vulnerable point of the network. If the CA is compromised, the security of the entire network is crashed. In [10], a threshold cryptography is used to provide robust and ubiquitous security support for the ad hoc networks. The CA functions are distributed through a threshold secret sharing mechanism. This approach is very complicated to implement. It is also hard to survive from multiple hijacked nodes that have secret shares.

IV. Proposed Solution

Key management is the process by which cryptographic keys are generated, stored, protected, transferred, loaded, used, and destroyed. At the initial stage, the data packet will be transmitted from source to destination over transmission media using efficient cryptographic algorithm to encrypt the entire packet. Cryptography is the process used to make a meaningful message appear meaningless. An algorithm is a set of rules or procedures used to scramble, or encrypt the plaintext to produce Cipher text. The algorithm applies a key to text [14]. Encryption is the procedure that guarantees secrecy of the data exchanged. Any encryption algorithm depends on some key, and keys are normally generated during authentication phase, so the two phases are strictly connected [15]. In the proposed architecture, an extended flavor of link level encryption will be used to encrypt the entire data packet. The packet encryption algorithm at the originating site encrypts the entire packet . The key-id controls the behavior of encryption and decryption mechanism. It specifies the information as the encryption algorithm, the encryption block size, the error checking code and lifetime of the key.
This Algorithm is also implemented in C language & work properly

- **Encryption Algorithm**

An encryption algorithm at the source site will encrypted the entire packet. The packet will be encrypted with the help of a particular key. The key has 8 distinct blocks. With the help of these blocks encryption is performed. In case of successful encryption it transmit the packet.

- **Encryption Algorithm**

Step 1: Activate and Initialize the Packet Pi
Step 2: If Packet is < [MAX LIMIT]. //max limit is 32 bit
Convert the packet into its binary equivalent & decompose the packet.
Else Insert the Record of Invalid Packet in Forensic Database // if it exceeds from max limit
Step 3: Generate a EK key with 8 distinct blocks.
(a) 000= 'a',001= 'b', 010= 'c' ,011= 'd' ,100= 'e',101= 'f' ,110= 'g',111= 'h'
(b) Then Encrypted Packet EPK is generated using key EK. // with the help of program in c lang.
Step 4: Packet equipped for Transmission.

- **Implementation**

Here EK has 8 distinct blocks, according to the order they are 000,001,010,011,100,101,110,111. So we put according to key generation technique 000=a, 001=b, 010=c, 011=d,100=e,101=f,110=g,111=h that is 1st level identification marks.
We consider the plaintext P as "**Encrypt**". The stream of bits, S, representing P is as follows: 98798765493 as 000111010111000110010100000110101. Now S is decomposed into some block with 3 bits length (L = 3). These are 000,111,010,111,000,110,010,100,000,110,101. So here is no unchanged block, (UB = NULL).Number of distinct block is 8 (N = 8). Now we encrypt Pi. Here Pi is decomposed into 000= 'a',111= 'h', 010 = 'c', 111= 'h', 000= 'a', 110= 'g', 010 = 'c',100 = 'e' , 000 = 'a', 110 = 'g' ,101= 'f'.
After putting those values encrypted EPK is "ahchagceagf".

Encryption
****
Enter The Packet 98798765493
****
Original packet is: 000111010111000110010100000110101.
****
After encryption : "ahchagceagf"
****

- **Decryption and Intercept Detection Algorithm**

A decryption algorithm at the destination site will check the entire encrypted packet. The received packet will be of specific format and structure in which key is given. By analyzing the structure of encrypted packet, the location of key will be accessed and the packet can be decrypted. In case, there is an interception and packet is not matched after decrypting the Cipher text Cp, a record will be inserted in the forensic database. The pattern/behavior of intercepts will be analyzed using a forensic analyzer. In case of successful decryption and transmission of packet, an acknowledgement will be transmitted to the web based database where the source site can verify the delivery of message.

- **Decryption Algorithm**

Algorithm
Step 1: Receive the Encrypted Packet EPK
Step 2: Decrypt the packet with the help of key EK.
Step 3: After Decryption we obtain packet Si. // Si is name of packet
if Si=Pi.
Decryption Successful
Accept the Packet
else
Insert the Record of Corrupt Packet in Forensic Database
Implementation

From key, all information about encryption can be collected. From different segments of the key, it is come to know that there are 8 distinct blocks, found from the plain text; length of decomposed block is 3-bit . The 1st segment of the key says that length of unchanged block is 0 (zero).We receive a packet EPK that is "ahchagceagf". Now we Decrypt EPK. Here EPK is decomposed into 'a'= 000 , 'h' = 111, 'c' = 010 , 'h'= 111, 'a' = 000, 'g'= 110, 'c'= 010, 'e' = 100, 'a'= 000, 'g'= 110, 'f'= 101. After putting those values decrypted EPK is 000111010111000110010100000110101 is same as source bits stream, so obviously decrypted text "**Encrypt**" is same as plane text.

Example of Decryption Routine
****
Encrypted Packet is: "ahchagceagf"
****
After Decryption: 00011101011100011001010000011010 1
****

The implementation of the scheme has been incorporated in language C. Its results can be embedded to the existing MANET schemes. The packet format of the existing schemes can be changed to add this concept in route table entry. Proposal is to change the existing formats of AODV to adjust new factor of the algorithm. There are three main phases in this protocol: RREQ (Route Request) phase, RREP (Route Reply) phase and ERR (Route Errors) phase. The message types are also defined by the protocol scheme. No Changes will be made in REQ phase. It has been assumed that at the start all nodes are trusted and Route Request phase can be carried out as it is. This will reduce the overhead considerably. The changes will be made in Repair phase. Maximum effort is involved in repair phase.
Effort is on to simulate the proposed scheme on NS2. The process is still under testing conditions there is hope that new scheme will work well for security considerations. There may be some counter effects like; a slight drop in packet delivery ratio and a bit of increment in end to end delay. This reduction in packet delivery and increase in delay cannot be considered as demerit of the scheme, rather it is the cost to achieve the secured route.

V. Conclusion

An analytical study has been done for contemporary secured routing protocols for Adhoc networks. Key management, Ad-hoc routing of wireless Ad-hoc networks were discussed. Areas have been identified where further work can be done. Networks are facing challenges from increasing interceptions and cracking attempts through various sources. Adhoc networking is still a raw area of research as can be seen with the problems that exist in these networks and the emerging solutions. 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 thwart such threats. Because the solutions are designed especially with certain attack models in mind, they work well in the presence of designated attacks but may collapse under unanticipated attacks. The key management protocols are still very expensive and not fail safe. Several protocols for routing in Ad-hoc networks have been proposed. There is a need to make them more secure and robust to adapt to the demanding requirements.

REFERENCES

[1] R. Hauser, A. Przygienda and G. Tsudik, "Reducing the cost of security in link state routing", In Symposium on Network and Distributed Systems Security (NDSS ˝97), San Diego, California, Internet Society, pp 93–99, February 1997.
[2] A. Kush, "Security Aspects in AD hoc Routing" , Computer Society of India Communications, Vol. 3 No 2 Issue 11, pp 29-33, March 2009.
[3] A. 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, June 2009.
[4] T. Karygiannis and L. Owens, "Wireless Network Security", NIST Special Publication, pp 800-848, November 2002.
[5] Yonguang Zhang and Wenke Lee, "Intrusion detection in wireless ad-hoc networks", In 6th International Conference on Mobile Computing and Networking (MOBICOM˝00), pp 275– 283, August 2000.
[6] A. Kush, C. Hwang and P. Gupta, "Secured Routing Scheme for Adhoc Networks" International Journal of Computer Theory and Engineering (IJCTE), Volume 3, pp 1793-1799, May 2009.
[7] Sonia Boora, Yogesh Kumar and Bhawna Kochar A Survey on Security Issues in Mobile Ad-hoc Networks IJCSMS International Journal of Computer Science and Management Studies, Vol. 11, Issue 02, Aug 2011 ISSN (Online): 2231-5268
[8] Panagiotis Papadimitratos and Zygmunt J. Haas, "Secure message transmission in mobile ad hoc networks", Elsevier Journal of Adhoc network, Ad Hoc Networks 1, pp 193–209, 2003.
[9] Fei Hu and Neeraj K. Sharma, "Security considerations in ad hoc sensor networks" Elsevier Journal of Ad hoc Networks, Ad Hoc Networks 3, pp 69–89, 2005.
[10] Jiejun-K, Petros-Z, Haiyun-Luo, Songwu-Lu, Lixia-Zhang. Providing robust and ubiquitous security support for mobile ad-hoc networks. Proceedings Ninth International Conference on Network Protocols. ICNP 2001, Riverside, CA, USA, 11-14 Nov. 2001.
[11] L. Zhou, Z. J. Haas. Securing Ad Hoc Networks. IEEE Network, 13(6): 24-30, Nov/Dec 1999.
[12] Perkins C.E., Das S.R. and Royer E.. Ad-hoc on-demand distance vector (aodv) routing. http://www.ietf.org/internet-drafts/draft-ietf-manet-aodv-05.txt, 2000 (accessed on May 03, 2004).

[13] Karpijoki V., Signaling and routing security in mobile and ad-hocnetworks.http://www.hut.fi/vkarpijo/iwork00/, 2000 (accessed on May 03, 2004).
[14] Youlu Zheng and Shakil Akhtar, "Networks for Computer Scientists and Engineers", Oxford University Press, 2009.
[15] Dimitris M. Kyriazanos, Neeli R. Prasad and Charalampos Z. Patrikakis, "A Security, Privacy and Trust Architecture for Wireless Sensor Networks", 50th International Symposium ELMAR-2008, Zadar, Croatia, pp 10-12, September 2008.
[16] Mohammad Al-Shurman and Seong-Moo Yoo, Seungjin Park, "Black Hole Attack in Mobile Ad Hoc Networks" ACMSE'04, April 2-3, 2004, Huntsville, AL, USA.
[17] Yih-Chun Hu, Adrian Perrig, and David B. Johnson., "Packet Leashes A Defense against Wormhole Attacks in Wireless Ad Hoc Networks" In Proceedings of the Twenty-Second Annual Joint Conference of the IEEE Computer and Communications Societies (INFOCOM 2003), April 2003. To appear.
[18] Patroklos g. Argyroudis and donal o'mahony, "Secure Routing for Mobile Ad hoc Networks", IEEE Communications Surveys & Tutorials Third Quarter 2005.
[19] I. Aad, J.-P. Hubaux, and E-W. Knightly, "Denial of Service Resilience in Ad Hoc Networks,"Proc. MobiCom, 2004.
[20] Yih-Chun Hu, Adrian Perrig, David B. Johnson, "Rushing Attacks and Defense in Wireless Ad Hoc Network Routing Protocols" WiSe 2003, September 19, 2003, San Diego, California, USA.
[21] Perkins C.E. and Royer E., Ad-hoc on-demand distance vector routing. In 2nd IEEE Workshop on Mobile Computing Systems and Applications, pages 90–100, 1999.
[22] Perkins C.E., Royer E.M., Das S.R., Ad hoc On- Demand Distance Vector (AODV) Routing .draft-ietfmanet-aodv-08.txt, March 2001.
[23] Broch J., Maltz D.A., Johnson D.B., Hu Y.C., and Jetcheva J., A performance comparison of multi-hop wireless ad hoc network routing protocols. In 4th International Conference on Mobile Computing and Networking (ACM MOBICOM' 98), pages 85–97, Oct 1998.
[24] Rahman A., Security issues in mobile systems, http://www.cs.ucl.ac.uk/staff/F.AbdulRahman/docs /sec-inob.html, 1995 (accessed on May 03, 2004).
[25] Jonny Karlsson , Laurence S. Dooley and Göran Pulkkis. Routing Security in Mobile Ad-hoc Networks in Issues in Informing Science and Information Technology Volume 9, 2012