Encryption Scheme for Secure Routing in Ad Hoc Networks

Sunil Taneja[1], Ashwani Kush[2] and Sima Singh[3]

[1]Department of Computer Science, Smt. Aruna Asaf Ali Government Post Graduate College,
Kalka, Haryana, India, suniltaneja.iitd@gmail.com

[2]Department of Computer Science, University College,
Kurukshetra University, Kurukshetra, Haryana, India, akush20@gmail.com

[3]Department of Computer Science, Karnal Institute of Technology & Management,
Karnal, Haryana, India, simasingh.2009@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. The key issues concerning these areas have been addressed here. 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

1. Introduction

Recent years have witnessed a proliferation of mobile devices. Corporations and government agencies alike are increasingly using embedded and wireless technologies. An Ad hoc wireless network is a collection of mobile devices equipped with interfaces and networking capability. It is adaptive in nature and is self organizing. A formed network can be de-formed and again formed on the fly and this can be done without the help of system administration. Each node may be capable of acting as a router. Applications include but are not limited to virtual classrooms, military communications, emergency search and rescue operations, data acquisition in hostile environments, communications set up in exhibitions, conferences and meetings, in battle field among soldiers to coordinate defence or attack, at airport terminals for workers to share files etc. Although security has long been an active research topic in wired networks, the unique characteristics of Ad Hoc networks present a new set of nontrivial challenges to security design. These challenges include open network architecture, shared wireless medium, stringent resource constraints, and highly dynamic topology. 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].

2. Mobile Adhoc Network: Attacks

These attacks can be broadly classified into two main categories as: Passive attacks and Active attacks.

2.1 Passive Attacks

Passive attacks are the attacks in which an attacker does not actively participate in bringing the network down. An attacker just eavesdrops on the network traffic as to determine which nodes are trying to establish routes, or which nodes are pivotal to proper operation of the network and hence can be potential candidates for subversion and launching denial of service attacks. The attacker can then forward this information to an accomplice who in turn can use it to launch attacks to bring down the network. 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 are:

1. *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.
2. *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.
3. *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.
4. *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.

2.2 Active Attacks

These attacks involve some modification of the data stream or the creation of a false stream and can be subdivided into four categories.

1. *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. An impersonate attack usually includes one of the other forms of active attacks.

2. *Replay:* This involves capture of data units and its subsequent retransmission to produce an unauthorized effect. Sniffers are used for legitimate network management functions.

3. *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.

4. *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. It is like shutting down a server that could not otherwise be compromised.

It is quite difficult to prevent active attacks absolutely, as this would require physical protection of all communications facilities and paths at all times. Instead, the goal is to detect them and to recover from any disruption or delays caused by them.

2.2 Intrusion Detection Schemes

MANETs present a number of unique problems for Intrusion Detection Systems [5](IDS). Differentiating between malicious network activity and spurious, but typical, problems associated with an ad hoc networking environment is a challenging task. In an ad hoc network, malicious nodes may enter and leave the immediate radio transmission range at random intervals or may collude with other malicious nodes to disrupt network activity and avoid detection. Malicious nodes may behave maliciously only intermittently, further complicating their detection. The loss or capture of unattended sensors and personal computing devices may allow for a malicious node to obtain legitimate credentials and launch more serious attacks. A node that sends out false routing information could be a compromised node, or merely a node that has a temporarily stale routing table due to volatile physical conditions. Dynamic topologies make it difficult to obtain a global view of the network and any approximation can become quickly outdated. Traffic monitoring in wired networks is usually performed at switches, routers and gateways, but an ad hoc network does not have these types of network elements where the IDS can collect audit data for the entire network. A wired network under a single administrative domain allows for discovery, repair, response, and forensics of suspicious nodes. A MANET is most likely not under a single administrative domain, making it difficult to perform any kind of centralized management or control.

3. Recent Work

Despite the fact that security of Ad Hoc routing protocols is causing a major roadblock in commercial application of this technology, only a limited work has been done in this area. Such efforts have mostly concentrated on the aspect of data forwarding, disregarding the aspect of topology discovery. On the other hand, solutions that target route discovery have been based on approaches for fixed-infrastructure networks, defying the particular ad hoc network challenges. Dahill et al. proposed ARAN [10], It assumes managed-open environment, where there is a possibility for pre-deployment of infrastructure. It consists of two distinct stages. The first stage is the certification and end-to-end authentication stage. Here the source gets a certificate from the trusted certification server, and then using this certificate, signs the request packet. Each intermediate node in turn signs the request with its certificate. The destination then verifies each of the certificates, thus the source gets authenticated and so do the intermediate nodes. The destination node then sends the reply along the route reverse to the one in the request; reply signed using the certificate of the destination. The second stage is a non-mandatory stage used to discover the shortest path to the destination, but this stage is computationally expensive. It is prone to reply attacks using error messages unless the nodes have time synchronization. Papadimitratos and Haas [7] proposed a protocol (SRP) that can be applied to several existing routing protocols. This protocol assumes a security association between source and destination nodes. Intermediate nodes do not need to cryptographically validate the control traffic. It adds a SRP header to the base routing protocol (DSR or AODV) request packet. SRP header has three important fields—QSEQ which helps prevent replay of old outdated requests, QID and random number which helps prevent fabrication of requests, and a SRP MAC which ensures integrity of the packets in transit. SRP requires that, for every route discovery, source and destination must have a security association between them. Furthermore, the paper does not even mention route error messages. Therefore, they are not protected, and any malicious node can just forge error messages with other nodes as source. ARIADNE [11], is based on DSR [13] and TESLA [12] (on which it is based its authentication mechanism). ARIADNE prevents attackers/compromised nodes from disrupting uncompromised routes comprising of benign nodes. It uses highly efficient symmetric key cryptography. ARIADNE does not guard against passive attackers eavesdropping on the network traffic. It does not prevent an attacker from inserting data packets. ARIADNE is vulnerable to active-1-1 attacker that lies along the discovered route, who does not forward packets and does not generate ERROR if it encounters a broken link. It also requires clock synchronization, which we consider to be an unrealistic requirement for ad hoc networks. Perlman proposed a link state routing protocol [14] that achieves Byzantine Robustness. Although the protocol is highly robust, it requires a very high overhead associated with public key encryption. In their paper on securing ad hoc networks [15], Zhou and Haas primarily discussed key management. They devote a section to secure routing, but essentially conclude that “nodes can protect routing information in the same way they protect data traffic”. They also observe that denial-of-service attacks against routing will be treated as damage and routed around. Some work has been done to secure ad hoc networks by using misbehavior detection schemes [16]. This approach has two main problems: first, it is quite likely that it will be not feasible to detect several kinds of misbehaving; and second has no real means to guarantee the integrity and authentication of the routing messages.

Looking at the work that has been done in this area previously, it seems that the security needs for adhoc networks has not been yet satisfied.

4. 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 Ciphertext. The algorithm applies a key to text [17]. 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 [18]. 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 including the packet header and provides it a new header. This readable new header also includes a dynamic key-id. 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.

Encryption Algorithm

```
Step 1: Activate and Initialize the Packet $P_i$
Step 2: Generate a Random Key $K_R$ by analyzing number of 1s in Packet.
    (a) Develop a routine to count bits in the Data Packet
    (b) Set N := Count($P_i$)      // Count Number of 1's in the Data Packet.
    (c) Set $K_R$ :=N              // Store N in Random Number $K_R$
Step 3: Apply XOR (Exclusive-OR) Operation
    (a) Set $E_K \oplus := P_i \quad K_R$
    (b) The Encrypted Packet $E_K$ is generated using XOR Operation.
    (c) Set $PE_K := E_K$          // Utilize $E_K$ as Encrypted Packet
Step 4: Packet equipped for Transmission
```

Example of Encryption Routine

Suppose we have a Data Packet with following Bit Stream –

10101010 10001000 00001010 11101010

The packet is represented as a 4 Byte or 32 Bits Data Packet.
Numbers of 1's in each byte are: 4, 2, 2, 5
Binary Equivalent of 4, 2, 2, 5 are 0100, 0010, 0010, 0101

Bitwise XOR Operation for Encryption of Packet

Actual Packet
10101010 10001000 00001010 11101010
Key
00000100 00000010 00000010 00000101

Encrypted Packet
10101110 10001010 00001000 11101111

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 of interceptions at the transmission line, the details of such attempts will be stored in the web based databases so that interception points and sources can be identified. In case, there is an interception and packet is not matched after decrypting the Ciphertext C_p, 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.

Algorithm

```
Step 1: Receive the Encrypted Packet $PE_K$
Step 2: Check the Front $PF_i$ and Rear End $PR_i$ of Packet
        if ($PF_i = PR_i$)
        Accept PFi
        Set $K_R := PF_i$
        else
        goto Step 5
Step 3: Generate the Binary Equivalent of $K_R$
        $PB_i = Binary(K_R)$
Step 4: Perform XOR Operation
        if ($PB_i = PE_K$)
                Decryption Successful
                Accept the Packet
        else
                goto step 5
Step 5: Insert the Record of Corrupt Packet in Forensic Database
```

Example of Decryption Routine

Key
0000100 00000010 00000010 00000101
Encrypted Packet
10101110 10001010 00001000 11101111

Actual Packet
10101010 10001000 00001010 11101010

The packet format of the existing schemes can be changed to add this concept in route table entry. The proposed algorithm will be incorporated on AODV. 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. The changed format has been shown in Appendix –I. In that the proposed format of key will change. In the New scheme format has been shown as ‘Secured new’. Cryptic key, Decrypted Key has been generated using the algorithm described above.

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. Local repair is carried out in AODV and the new scheme will first incorporate this algorithm before selection of new route. The route table entry will be modified and reply nodes will give assurance of secure route. Hello messages will bacon with updated route table entries. This process may delay the route selection a bit but this will make the route more trustworthy. More computational efforts may also affect packet delivery.

Effort is on to simulate the proposed scheme on NS2. The process is still under testing stages and there is hope that new scheme will work well for security considerations with 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. The scheme should work well for mobile ad hoc networks with large number of nodes. More nodes provide flexibility in route selection in repair mode. It can handle low, moderate, and relatively high mobility rates. It can handle a variety of data traffic levels.

5. Conclusion

An analytical study has been done for contemporary secured routing protocols for Adhoc networks. Areas have been identified where further work can be done. Networks are facing challenges from increasing interceptions and cracking attempts through various sources. There is need to secure the data packets roaming around the network from multiple interceptions using efficient cryptographic algorithms. The packet encryption algorithm explained in the paper is an efficient algorithm based on Exclusive-OR operation which is a unique method. Using this method, encryption and decryption can be performed effectively with unique cryptographic technique without any complexity. Moreover, the forensic database will keep record of every invalid or unacceptable decrypted packet. Using records in this database, one can analyze the behavior of intercepts to avoid these in future. Efforts are on to simulate the proposed scheme with different topologies and trying to compare it with existing secured routing schemes. 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 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. Therefore, a more ambitious goal for ad hoc network security is to develop a multifence security solution that is embedded into possibly every component in the network, resulting in in-depth protection that offers multiple lines of defense against many both known and unknown security threats.

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] 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), January 2002.

[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] B. 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, August 2001.

[11] Y. C. Hu, A. Perrig and D. B. Johnson, “Ariadne: A secure on-demand routing protocol for ad hoc networks”, Technical Report TR01-383, Rice University, December 2001.

[12] A. Perrig, R. Canetti, D. Song and D. Tygar, “Efficient and secure source authentication for multicast”, In Network and Distributed System Security Symposium (NDSS’01), February 2001.

[13] D. B. Johnson et al., “The dynamic source routing protocol for mobile ad hoc networks (DSR)”, Internet Draft, MANET working group, February 2002.

[14] R. Perlman, “Fault-tolerant broadcast of routing information”, In Computer Networks, No. *7*, pp 395–405.

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

[16] S. Marti, T. J. Giuli, K. Lai and M. Baker, “Mitigating routing misbehavior in mobile ad hoc networks”, In Proceedings of the Sixth Annual International Conference on Mobile Computing and Networking, pp 255–265, 2000.

[17] Youlu Zheng and Shakil Akhtar, “Networks for Computer Scientists and Engineers”, Oxford University Press, 2009.

[18] 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.

Appendix –I

Route Request Formats:

AODV Request

AODV REQ
Type Flag Hop Count
REQ ID DEST IP SRC IP

Secured New

NEW REQ
Type Flag Hop Count
REQ ID DEST IP SRC IP
Cryptic key, Decrypted Key

Route Reply Formats:

AODV Reply

Type FLAG Hop Count
Destination IP Address, Source IP Address

Secured New

Type FLAG Hop Count
Destination IP Address, Source IP Address,
Cryptic Key, Decryptic Key