Journal of Applied Sciences

ISSN 1812-5654

science alert

ANSInet
an open access publisher
http://ansinet.com

Journal of Applied Sciences 7 (24): 4007-4012, 2007
ISSN 1812-5654

Data Security in Ad Hoc Networks Using Randomization of Cryptographic Algorithms

[1]B. Ananda Krishna, [1]S. Radha and [2]K. Chenna Keshava Reddy
[1]Department of ECE, SSN College of Engineering, SSN Nagar, Kalavakkam-603 110, India
[2]Department of ECE, JNTU, Kukatpally, Hyderabad-500 072, 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. Instead, hosts rely on each other to keep the network connected. The military tactical and other security-sensitive operations are still the main applications of ad hoc networks, although there is a trend to adopt ad hoc networks for commercial uses due to their unique properties. One main challenge in design of these networks is how to feasibly detect and defend the major attacks against data, impersonation and unauthorized data modification. Also, in the same network some nodes may be malicious whose objective is to degrade the network performance. In this study, we propose a security model in which the packets are encrypted and decrypted using multiple algorithms where the selection scheme is random. The performance of the proposed model is analyzed and it is observed that there is no increase in control overhead but a slight delay is introduced due to the encryption process. We conclude that the proposed security model works well for heavily loaded networks with high mobility and can be extended for more cryptographic algorithms.

Key words: Security, encryption, decryption, randomization, MANETs, CBR traffic

INTRODUCTION

A Mobile Ad hoc Networks (MANETs) are a new paradigm of wireless communication for mobile hosts (nodes) and an autonomous system without any fixed infrastructure such as base stations or mobile switching centers. Mobile nodes that are within each other's radio range communicate directly via wireless links, while those that are far apart rely on other nodes to relay messages as routers. Node mobility in an ad hoc network causes frequent changes of the network topology. This fact creates many challenging research issues such as routing, allocation resources like bandwidth, battery power, security and other types of QoS.

Today, military tactical operations are the main application of ad hoc networks. For example, military units (e.g., soldiers, tanks or planes), equipped with wireless communication devices, could form an ad hoc network when they roam in a battlefield. Ad hoc networks can also be used for emergency, law enforcement and rescue missions. 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.

Security goals: Security is an important issue (Zhou and Haas, 1999) for ad hoc networks, especially for security sensitive applications. In order to analyze security (and security attacks) of a network, we need to know the basic requirements for a secure system are confidentiality, integrity, availability, authenticity, accountability and non-repudiation.

Challenges: The salient features of ad hoc networks pose both challenges and opportunities in achieving these security goals.

First, use of wireless links renders an ad hoc network susceptible to link attacks ranging from passive eavesdropping to active impersonation, message replay and message distortion. Eavesdropping might give an adversary access to secret information, violating confidentiality. Active attacks might allow the adversary to delete messages, to inject erroneous messages, to modify messages and to impersonate a node, thus violating availability, integrity, authentication and non-repudiation. The cryptanalytic attacks depend on nature of the algorithm, knowledge of the general characteristics of the plain text and sample plain text-cipher text pairs. Therefore, to achieve high survivability, ad hoc networks should have strong cryptographic algorithms for data security. Instead of using single cryptographic algorithm we introduced random selection of multiple cryptographic algorithms (Sharanya *et al*., 2007) in our security model to improvise the existing data security approaches to suit technology enhancements.

Corresponding Author: B. Ananda Krishna, Department of ECE, SSN, College of Engineering, SSN Nagar, Kalavakkam-603 110, India

Secondly, nodes, roaming in a hostile environment (e.g., a battlefield) with relatively poor physical protection, have non-negligible probability of being compromised. Therefore, we should not only consider malicious attacks from outside a network, but also take into account the attacks launched from within the network by compromised nodes.

Finally, an ad hoc network may consist of hundreds or even thousands of nodes. Security mechanisms should be scalable to handle such a large network.

Scope and roadmap: Traditional security mechanisms, such as authentication protocols, digital signature and encryption, still play important roles in achieving confidentiality, integrity, authentication and non-repudiation of communication in ad hoc networks. However, these mechanisms are not sufficient by themselves.

For example, in the symmetric key cryptography, if attacker discovers the key and knows the algorithm with any one of the attacks, all the communication between source and destination is readable. Therefore, to strength the encryption algorithm and key, first we take the advantage of random selection of cryptographic algorithms. Second, our intention is to achieve security by using simple algorithms that involve small inherent delays rather than resorting to complex algorithms, which occupy considerable memory and delays.

Secure ad hoc routing protocols have been proposed as a technique to enhance the security in MANET. Yih-Chun *et al.* (2002a) proposed a common key encryptosystem to Dynamic Source Routing (DSR). Secure AODV (SAODV) (Zapata, 2005) and Secure Efficient Ad hoc Distance Vector Routing Protocol (Yih-Chun *et al*., 2002b) are examples of the secure routing protocols using hash-based functions. Also several approaches such as reputation based schemes and watchdog mechanisms have been proposed in the literature to help the detection process in Intrusions Detection Systems (Michiardi and Molva, 2002; Marti *et al*., 2000). Kachirski and Guha (2003) proposed the idea of distributed IDS where cluster heads are elected and the IDS functionality is distributed among them. Many complex encryption algorithms (Stallings, 2004) have been proposed such as RSA, DES, etc. for wired networks. In spite of processing a huge key size and a series of complex manipulations of the plaintext these algorithms are not secure. It requires high memory, cost and processing time. Hence their use in small time applications is not resourceful. Also, a keen study of the cipher text samples would reveal a conspicuous pattern because of the continual nature of the responses. For example e is the frequently occurring letter among all alphabets. Hence frequently occurring letters in a cipher text can be replaced by e. Such a continual substitution would finally lead to the plain text. In this study, we state a method of random selection of simple cryptographic algorithms with small inherent delays, the response would yield a random pattern that overcomes the frequency analysis and the performance of the network is studied by simulation. In this study, we do not focus on how to defend against security attacks and focus on performance of the network.

SECURITY USING RANDOMIZATION OF CRYPTOGRAPHIC ALGORITHMS

The main objective of proposed security model is to improvise the existing data security approaches for MANETs to suit technology enhancements and to study the network performance. In this model we use multiple algorithms like algorithm 1, algorithm 2 and algorithm 3 and so on for encryption and decryption process. Each time a data packet is sent to the application layer and it is encrypted using one of these algorithms, which is selected randomly. The random selection of encryption and decryption algorithm is shown in Fig. 1 and 2. For example, for the first transmitted packet an algorithm 1 is selected. For the next packet, it may be algorithm 2 or algorithm 3 or even algorithm 1. When responses are analyzed they will give a random pattern and difficult to know neither algorithms nor keys.

Both the sending and receiving end agree upon a common set of algorithms used for encryption and decryption of the data packets. To properly coordinate the decryption on the other end, an appropriate synchronizing function is chosen. Each of the response follows a different encryption scheme and thus bears no

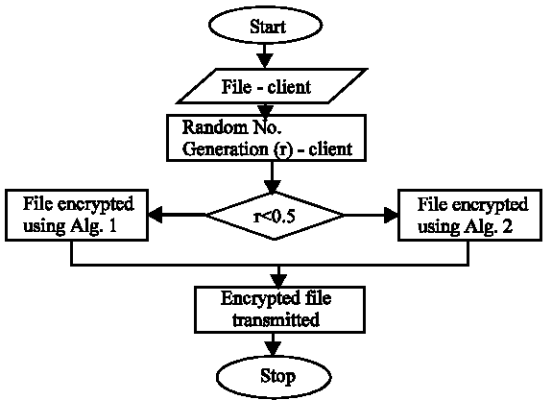

Fig. 1: Encryption process

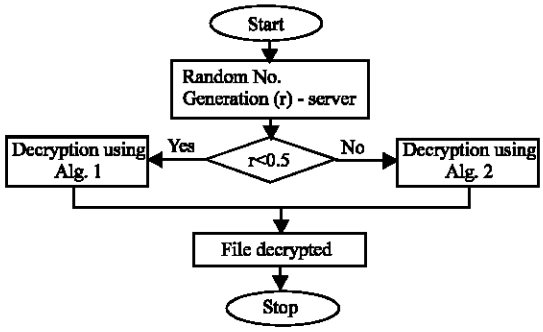

Fig. 2: Decryption process

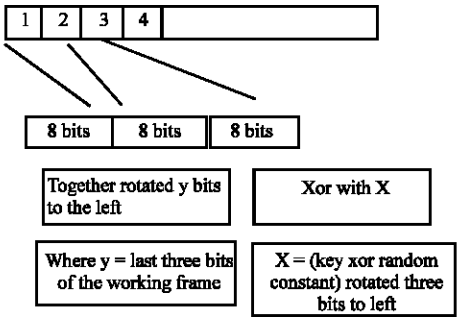

Fig. 3: Working frame in encryption

resemblance with one another (Fig. 3). Hence the samples of the cipher text upon any kind of comparisons would not yield any similarity. The proposed work is implemented using two conventional algorithms, which can overcome the passive attacks, cryptanalysis and brute force analysis (Stallings, 2004) and this model can be extended to any number of algorithms.

OVERVIEW OF CRYPTOGRAPHIC ALGORITHMS

Here, we discuss the overview of the proposed simple algorithms namely R-XOR algorithm and Fiestel algorithm used for the data security in Mobile Ad hoc Networks using Ad hoc On demand Distance Vector (AODV) protocol (Radha and Rajkumar, 2005).

R-XOR algorithm: The first simple algorithm is performing Rotations and XOR (R-XOR) operations; this algorithm rotates the data either left or right and then XORed with a key. For example consider a 3-bytes of the data called as working frame in which the first 2 bytes are together rotated a variable number of positions while the last byte is XORed with key. Also the key is XORed with a random number. This makes the entire process reversible since it contains only XOR and rotations.

Algorithm for Encryption

1. XOR the entire key with the random constant and then rotate to the 3 bits lefts.
2. Rotate the first two bytes of the working frame to three bits to the left.
3. XOR the lower-order byte of the working frame with the lower order byte of the key.
4. Shift the working frame to 3bits to the left and repeat the process for the entire frame.
5. Length of the constant must be equal to the length of the key.

Algorithm for Decryption

1. The working frame starts the 3rd to last byte of the cipher text and advances in the reverse direction circularly through to the 2nd to last byte of the cipher text.
2. Both the key and 2 cipher text bytes are shifted to the right.
3. Do XOR before rotations.

Fiestel algorithm: In this algorithm, a block of size N (where N is even) is divided into two halves (of length N/2) left half called XL and right half called XR. The block is iterated i.e., the output of the ith round is determined from the output of the (i-1)th round. We used only one key for all iterations without generating sub keys. Also the number of rounds the iterations are performed has been reduced, as our whole intent is to show that security can be achieved by using simple algorithms. The Plaintext is divided into blocks of 512 bytes. Encryption is performed for every 32 bits and the iteration is repeated until all 512 bytes of plaintext are encrypted.

Algorithm for Encryption and Decryption

1. Divide the plaintext (32 bytes taken at a time) into two blocks of size 16 bytes, XL and XR.
2. For i = 1 to 16
   Do XL = XL XOR KEY
   XR = F (XL) XOR XR
   Swap XL, XR
   Join XL, XR
3. Repeat step 2 (32 times) until the entire plaintext is encrypted.
4. Repeat the reverse operation for decryption.

EVALUATION OF IMPLEMENTATION AND SIMULATION

In order to evaluate the network performance of the proposed security mechanism, ad hoc network is simulated using Global Mobile Information System (GloMoSim) Simulator (Nuevo, 2004). It is a scalable simulation environment for large wireless network systems and uses a parallel discrete-event simulation capability provided by C-based Parallel Simulation Environment for Complex systems (Parsec).

Table 1: Simulation parameter

Simulation area	2000×2000
No. of nodes	100
MAC layer	802.11
Transport layer	UDP and TCP
Traffic	CBR traffic
Mobility model	Random waypoint
Node placement	Uniform
Routing protocol	AODV
Simulation time	600 sec

Implementation parameters: The simulations were based on 2000 by 2000 m flat space scattered with 100 wireless nodes and IEEE 802.11 wireless LAN standard was used as the MAC protocol. The random waypoint mobility model is used for the node mobility in which a node selects a destination randomly within the simulated territory, moves to that destination as speed uniformly distributed in (V_{min}, V_{max}) m sec^{-1} and stops there for a predefined pause time and then repeats this behavior for the entire duration of the simulation. The default simulation parameters were shown in Table 1.

To evaluate the performance of the data security the following parameters were analyzed.

Average throughput: The ratio of data packets delivered to the destinations to data packets originated by the sources. This number presents the routing efficiency of the protocol.

Packet delivery ratio: The ratio of the data packets delivered to the receivers to those data packets expected to be delivered

End-to-end delay: The end-to-end delay counts the time interval from the moment that the source node sends a first message until the moment that the destination node in the network receives this last message. It also includes all possible delays caused by queuing at the interface, retransmission delays and propagation and transfer times.

Control overhead: The control overhead includes the number of control packets transmitted by all the nodes during the entire simulation.

Total overhead: The ratio of the total packets transmitted (i.e., sum of control packets and data packets) to the data packets delivered.

SIMULATION RESULTS

The simulation results obtained by comparing with different speed and different traffic.

Figure 4 shows the comparison of control overhead various network traffic for high mobility network. From the graph it is observed that as the overall traffic in the network increases the control overhead increases by a route discovery process and is mainly due to the number of route requests flooded in the network. From the graph we observe that when the speed of the mobile node is increases from 1 to 20 m sec^{-1}, then the control overhead proportionally increases from 1 to 46.8%. This is mainly due to the frequent route failures, which in turn increases the number of route discovery process.

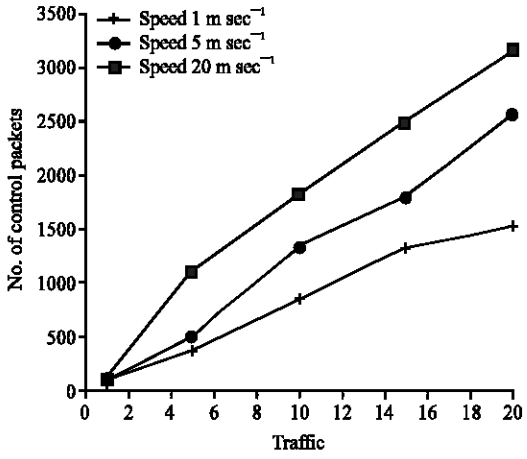

Fig. 4: Number of control packets vs traffic

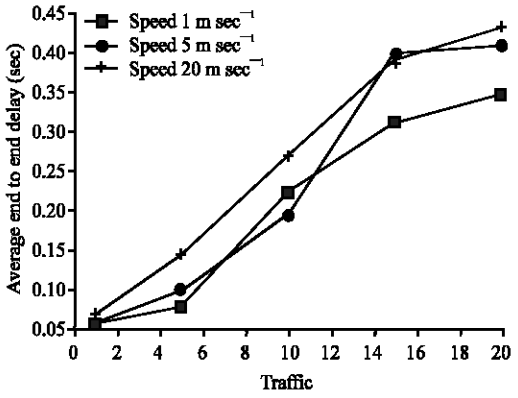

Fig. 5: Average end-to-end delay vs traffic

Figure 5 shows the average end-to-end delay of the data encrypted scheme, which is defined to be the interval between the time when a source node initiates the data packet and the time when the destination node receives the last data packets. From the graph, we observe that as mobility increases the delay increases, mainly due to the retransmission of data packets because of route failures.

The performance of packet delivery ratio as the number of sender in the network increases under different mobility is as shown in Fig. 6. From the graph we can see that for low mobility, as the traffic increases the entire encrypted data packets are delivered successfully. For the

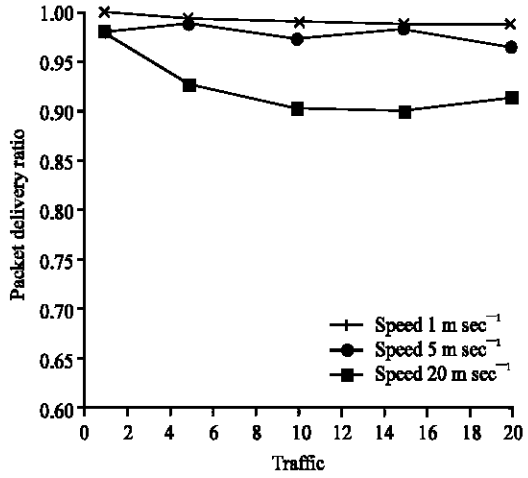

Fig. 6: Packet delivery ratio vs traffic

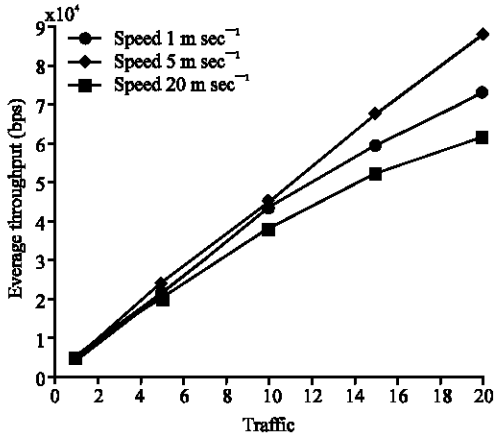

Fig. 7: Average throughput vs traffic

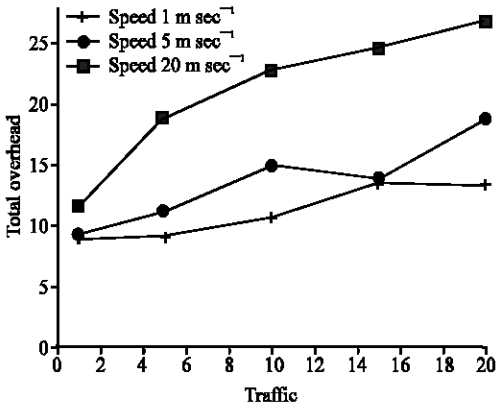

Fig. 8: Total control overhead vs traffic

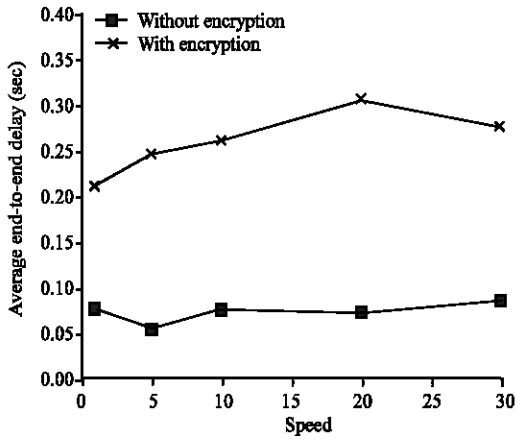

Fig. 9: Average end-to-end delay vs speed

medium mobility, as the traffic increases there is a small amount of dropping of data packets due to packet expire time due to route failures. Under high mobility, as the traffic increases the network drops nearly 8 to 10% of data packets as compared to low mobility scenario. This is mainly due to the frequent route failures and the packet expiration time out due to the delay of encryption and decryption process.

The Fig. 7 presents the average throughput of network under different traffic and mobility. It has observed initially for smaller values of mobility, the increase in delay is not significant. So throughput is almost a constant and the average throughput is increases to 90% as the traffic in the network increases for less speed and decreases to 69% as the speed increases from 1 to 20 m sec^{-1}. This is due to the number of collision increases as the traffic in the network increases and also packet dropping will be more as the route failure increases when the network speed increases. This number presents the routing efficiency of the protocol. As the mobility increases, delay increases as a result the probability of all packets delivered in time at the receiver decreases. Hence the average throughput decreases as the speed of the mobile increases.

The number of total control overhead is small for lower speed and increases to 64% more for higher speed than with low mobility as the traffic in the network increases from 1 to 20 (Fig. 8). This is due to the number of route failure increase as the speed of the mobile increases from 1 to 20 m sec^{-1}, which in turn increases the number of route discovery process.

Due to encryption a finite delay is introduced in the transmission of packets since the entire file is encrypted in the transmitted side and decrypted in the receiver side. The observed delay is found to be greater than compared to delay without encryption scheme. Initially delay

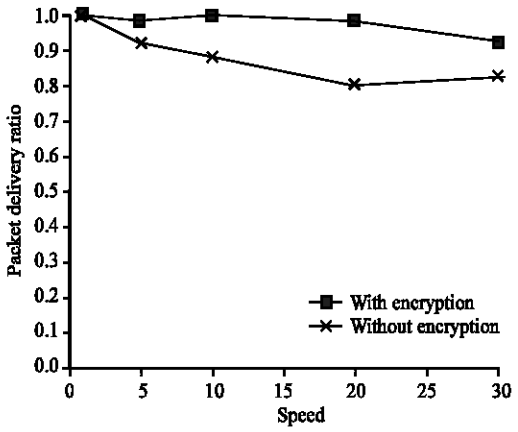

Fig. 10: Packet delivery ratio vs speed

decreases at lower mobility values, which may be attributed to the case when nodes come together. The delays of only the data packets that wait for route discovery increases where as delay for all other data packets are unaffected. Therefore the increase in the end-to-end delay is fairly constant (Fig. 9).

Figure 10 shows that throughput remains essentially constant for lower values of mobility, for higher values of mobility the packet delivery ratio increases to 90% compared to without encryption. We can infer that the data encryption techniques will not affect the average throughput as the traffic in the network as well as the speed of the mobile increases.

CONCLUSIONS

In this study, we have discussed a novel method for the data security in mobile ad hoc Network using randomization of selection of algorithms. The proposed methodology was investigated on the performance of AODV with CBR traffic. We have first analyzed the protocol performance with data security and compared the performance with and without encryption. The proposed security scheme shows that the packet delivery ratio increases to 90% as compared to data sent without encryption. From the results it is found that there is not much increase in control overhead as the traffic in the network increases but a slight delay is introduced due to the encryption process. From this study we conclude that the proposed randomized scheme was tested using only two algorithms for providing data security and works well for heavily loaded networks with high mobility.

REFERENCES

Kachirski, O. and R.K. Guha, 2003. Effective intrusion detection using multiple sensors in wireless ad hoc networks. HICSS, pp: 57.

Marti, S., T.J. Giuli, K. Lai and M. Baker, 2000. Mitigating routing misbehaviour in mobile ad hoc networks. Mobile Computing and Networking, pp: 255-265.

Michiardi, P. and R. Molva, 2002. Core: A collaborative reputation mechanism to enforce node cooperation in mobile ad hoc networks. Proceeding of Communication and Multimedia Security Conference.

Nuevo, J., 2004. A comprehensible glomosim tutorial. INRS-Universite du Quebec.

Radha, S. and S. Rajkumar, 2005. Enhanced intrusion detection algorithm for NTP based routing protocol for wireless ad hoc networks. IETE J. Res., 51: 351-359.

Sharanya, K., N. Subha, R.S. Ranjini, S. Radha and B.A. Krishna, 2007. Security enhancement in ad hoc networks using randomization of algorithms. Proc. IconADELCO 07, February 2007, pp: 47-52.

Stallings, W., 2004. Cryptography and Network Security-Principles and Practices. 3rd Edn., Person Education.

Yih-Chun, H., A. Perrig and D.B. Johnson, 2002a. Ariadne: A secure on-demand routing protocol for ad hoc networks. Proceedings of the 8th Annual International Conference on Mobile Computing and Networking (MobiCom 2002), pp: 12-23.

Yih-Chun, H., D.B. Johnson and A. Perrig, 2002b. SEAD: Secure efficient distance vector routing for mobile wireless ad hoc networks. Proceedings of 4th IEEE Workshop on Mobile Computing Systems and Applications, pp: 3-13.

Zapata, M.G., 2005. Secure Ad Hoc On-Demand Distance Vector (SAODV) routing. IETF Inter-net Draft. Draft-Guerrero-Manet-Saodv-03.

Zhou, L. and Z.J. Haas, 1999. Securing ad hoc networks. IEEE Network Magazine.