International Journal of Computer Networks and Communications Security

VOL. 2, NO. 12, DECEMBER 2014, 456–461
Available online at: www.ijcncs.org
ISSN 2308-9830

An Enhanced Data Security with Compression for MANETs

G.Soma Sekhar[1] and Dr.E.Sreenivasa Reddy[2]

[1] Research Scholar, Department of CSE, Acharya Nagarjuna University, Guntur

[2] Professor, College of Engineering, Acharya Nagarjuna University, Guntur

E-mail: [1]somasekharonline@yahoo.co.in, [2]esreddy67@gmail.com

ABSTRACT

Ad hoc networking is a wireless networking paradigm for self-organizing networks that until recently has mainly been associated with military battlefield networks. However, with the availability of wireless technologies such as Bluetooth and 802.11 and the development of the next generation networks, civilian applications that exploit the advantages of ad hoc networking are being envisioned. So far most of the research has been carried out to address the routing issues. Whereas other issues such as security, key management and network addressing have received considerably less attention and these issues need to be addressed before any successful applications will appear. In this paper, we propose a novel secured compression algorithm for an ad hoc network in which the packets are encrypted and compressed. The decompression and decryption using the same algorithm happens by a perfect synchronization between the sender and the receiver. It is observed that the proposed security concept may increase the level of confidence in this network.

Keywords: *Compression, Decompression, Encryption, Decryption, MANETs.*

1 INTRODUCTION

An ad hoc network is a collection of computers (nodes) that cooperate to forward packets for each other over a multi-hop wireless network. The nodes in the network may move and radio propagation conditions may change at any time, creating a dynamic, rapidly changing network topology. Ad hoc networks require no centralized administration or fixed network infrastructure such as base stations or access points, and can be quickly and inexpensively set up as needed. They can thus be used in scenarios where no infrastructure exists, or where the existing infrastructure does not meet application requirements for reasons such as security, cost, or quality. Security is an important issue for ad hoc networks, especially for security sensitive applications. In order to analyze security of a network, we need to know the basic requirements of a secure system such as confidentiality, integrity, availability, authenticity, accountability, and non- repudiation.

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 confidentiallity. 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.

Users of ad hoc networks may wish to use demanding applications such as videoconferencing, Voice over IP, and streaming media when they are connected through an ad hoc network. Quality of Service (QoS) has been an important area of research in wired networks, as researchers have looked for solutions that provide acceptable levels of performance for these types of applications. When QoS routing is available in ad hoc networks, users will experience better performance while using these types of challenging applications [1]. But there are some constraints in providing QoS such as Unpredictable Link Properties, Hidden Terminal Problem, Node Mobility, Route Maintenance, Limited Battery Life, Security etc.

There are many aspects to improve the battery life in which data compression technique is one [2]. This is achieved by transmitting the compressed data between the nodes (users) and retrieving the original data at the destination. For data compression we have many algorithms in which Lempel-Ziv- Welch (LZW) compression algorithm [3]-[5] is the best. LZW algorithm is efficient because the output resembles numerical data and also it

Doesn't need to pass the string table to the decompression code. Due to compression, the number of bits can be reduced to maximum extend so that the need of memory and bandwidth are very less. Also, the compressed text resembles a scramble message and an attacker in middle cannot able to understand. Therefore, the data compression not only reduces the size of the original text, but also gives data security.

Section 2 describes the security in Ad hoc Networks and section 3 describes motivation and proposed work. Section 4 describes the Simulation results and section 5 concludes.

2 RELATED WORK

The authors M. Madhurya, et al, proposed a novel security model for MANETS with the objective to achieve data confidentiality and authentication by novel cryptographic algorithm and also to secure the routing protocol by minimizing the malicious nodes. The proposed methodology was investigated on the performance of AODV with CBR traffic. They have analyzed the protocol performance with both data security as well as with Disturbance Detection Algorithm and proved that the performance of the network is increased [6].

The authors Wenjing Lou, et al., proposed a novel scheme, Security Protocol for REliable dAta Delivery (SPREAD), to enhance the data confidentiality service in a mobile ad hoc network. The proposed SPREAD scheme aims to provide further protection to secret messages from being compromised (or eavesdropped) when they are delivered across the insecure network. The basic idea is to transform a secret message into multiple shares by secret sharing schemes and then deliver the shares via multiple independent paths to the destination so that even if a small number of nodes that are used to relay the message shares are compromised, the secret message as a whole is not compromised. The simulation results show that SPREAD can provide more secure data transmission when messages are transmitted across the insecure network [7].

The Jigsaw Puzzle scheme addresses data confidentiality and integrity in a MANET environment [8]. Multipath routing is used to statistically enhance the confidentiality of exchanged messages between the source and destination nodes. The All-or-Nothing Transform is applied to a secret message to guarantee that no information can be obtained about the message unless all of its pieces are known. The message is then broken up into pieces by a jigsaw puzzle algorithm, which is based on operations with roots of polynomials. The pieces are transmitted across multiple node-disjoint paths. A Message Authentication Code (MAC) is transmitted with each piece to provide data integrity and origin authentication. Thus, it becomes impossible to compromise a secret message unless an adversary can eavesdrop close to the source or destination or simultaneously listen on all of the paths.

The authors B.Ruxanayasmin, et al, implemented a novel scheme to eliminate the redundant hardware as well as the redundant transformed data which reduces system complexity, memory, bandwidth and power. The proposed work is the combination of cryptography and compression algorithms. In the first stage, the incoming bit stream is divided into packets of size 128 bits each, and performs one‟s complement on the bits. The one‟s complemented data is XORed with secret key of 128 bit size. The encrypted text is compressed using LZW algorithm and transmitted. At receiver, the reverse operation is performed to get back the original data [9].

The authors Diaa Salama, et al, [10] proposed energy consumption of different common symmetric key encryptions on handheld devices. It is found that after only

600 encryptions of a 5 MB file using Triple- DES the remaining battery power is 45% and subsequent encryptions are not possible as the battery dies rapidly.

3 MOTIVATION & PROPOSED MODEL

In order to secure the ad hoc network, we proposed a security model with following motivation.

- Due to compression the Plain text may not be recognized when the encrypted data is uncovered in the brute force cryptanalysis.
- Compressed data packets are encrypted using cryptographic algorithms
- Due to compression technique the band-width efficiency increases.
- Compression decreases the power consum-ption, which increases the battery life [2].
- Encryption and decryption plays a vital role to secure data.
- To eliminate the redundant hardware as well as the redundant transformed data this reduces system complexity, memory, bandwidth and power.

The main objective of proposed model is to improvise the existing data security approaches for MANETs to suit technology enhancements and to study the network performance. In this model a simple cryptographic algorithm is combined with compression algorithm instead of using separate algorithms. Each time a data packet is sent to the application layer, it is encrypted and compressed using SLZW algorithm, and the reveres process is applied at receiver. When responses are analyzed they will give a random pattern and difficult to know neither algorithms nor keys. The proposed work is implemented using simple algorithms; to overcome the passive attacks, cryptanalysis and brute force analysis, and this model can be extended by increasing more number of iterations.

3.1 Secured LZW (SLZW) Algorithm

The SLZW algorithm is the combination of cryptography and compression techniques. In the first stage, the incoming bit stream is divided into packets of size 128 bits each, and performs encryption using a symmetric key. The encrypted text is compressed using LZW algorithm and transmitted. At receiver, the reverse operation is performed to get back the original data. By implementing this algorithm, we can

- Protect the information from attackers
- Reduce the memory usage and trans-mission bandwidth
- Transmitting less number of bits consumes less power

The Fig.1 shows the flowchart of the proposed work, in which simple cryptographic technique is combined with LZW algorithm and named as Secured LZW (SLZW) algorithm. It has minimum number of iterations and uur 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.

The principle in LZW is always tries to output codes for strings that are already known. And each time a new code is output, a new string is added to the string table

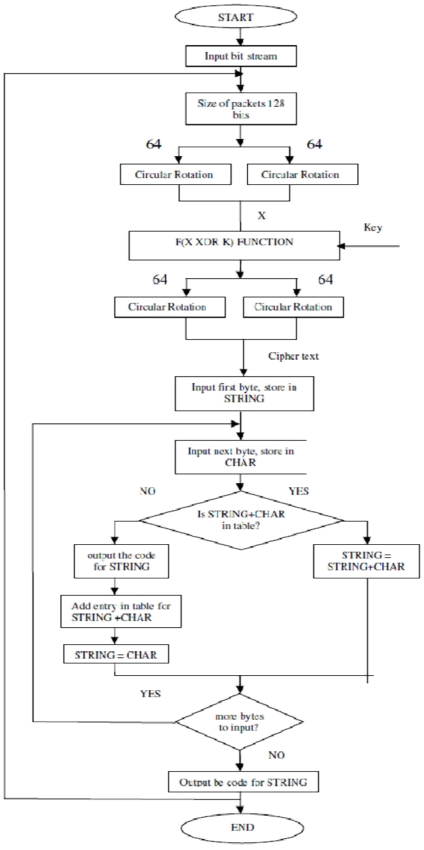

Fig. 1. SLZW Encryption Algorithm

The SLZW is the combination of cryptographic algorithm with compression technique. In this, the incoming data is data packets of size 128 bits and each packet is encrypted with SLZW. In the first iteration, the 128 bits are divided into two halves of 64 bits each and circular rotation (either left or right) is performed on each 64 bits. In the second iteration, the circularly rotated bits are combined into 128 bits and perform XOR operation with private key.

In the third iteration, the XORed 128 bits are divided into 64 bits and perform circular rotation. The output of third iteration is named as cipher text and it is compressed using LZW principle.

The decryption algorithm needs to be able to take the stream of codes output from the compression algorithm, and use them to exactly recreate the input stream as shown in Fig.2. One reason for the efficiency of the LZW algorithm is that it does not need to pass the string table to the decompression code. The table can be built exactly as it was during compression, using the input stream as data. This is possible because the compression algorithm always outputs the STRING and CHARACTER components of a code before it uses it in the output stream. This means that the compressed data is not burdened with carrying a large string translation table. After decompression, the data is decrypted with secret key yields the original data.

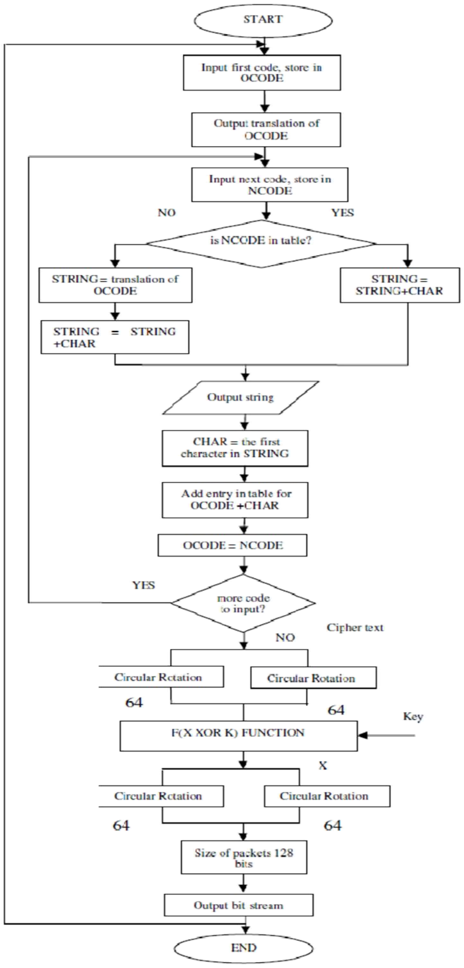

Fig. 2. SLZW Decryption Algorithm

4 RESULTS AND PERFORMANCE ANALYSIS

The proposed model is simulated using Glomosim simulator [11], implemented in AODV routing protocol. The simulation is done for a network having 50 mobile nodes, which move over an area of 1000 x 1000 m2 with a certain speed. Table 1 gives the system parameter values used in the analysis and simulations.

Table 1: Simulation Parameters

Simulation Time	**10 Min**
Bandwidth	**2 Mbps**
Frequency of	**2.4 GHz**
Simulation Area	**1000 m x 1000 m**
Number of Nodes	**50**
Offered Traffic	**12 packets/sec**
Radio Range	**250 meters**
Application	**CBR**
Transport	**TCP**
Network	**AODV**
MAC	**802.11**

4.1 Performance Evaluation

The following metrics were used to evaluate the performance of the data security. The following metrics are chosen to evaluate the efficiency in addition to the effectiveness of the protocols.

I. Packet Delivery Ratio (PDR): Measured as the ratio of the data packets delivered to the receivers to those data packets expected to be delivered.

II. (End-to-End Delay: Measured as 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.

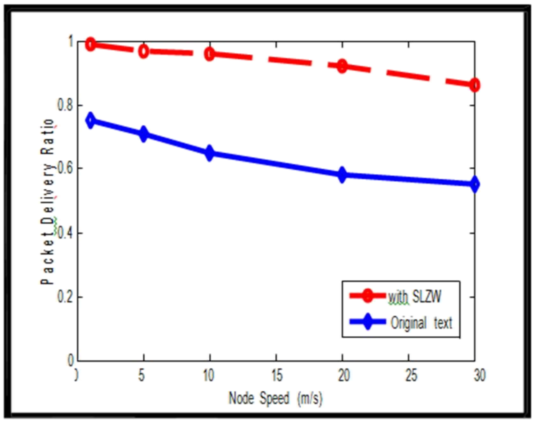

Fig. 3. Packet Delivery Ratio Vs Node Speed

The performance of packet delivery ratio under different speed is as shown in Fig.3. It is clearly shown for low speed; the routing protocol with SLZW delivers data packets successfully. For medium mobility, as the speed increases PDR slightly reduced due to packet dropping and further reduce for high speed. Whereas the PDR is much less when the data packets are transmitted without SLZW algorithm.

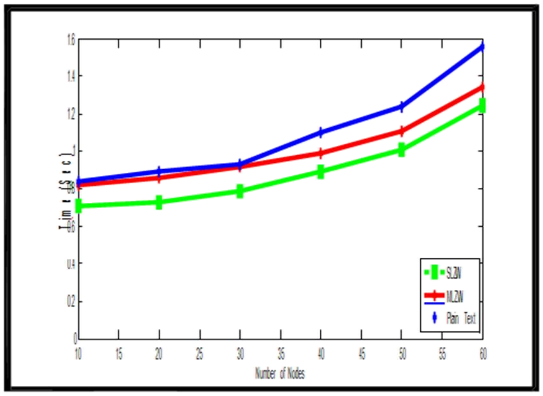

Fig. 4. Average end-to-end delay Vs Number of Nodes

Fig. 4 shows, the numbers of nodes through which the text is sent is plotted in the x- axis, where as time taken to transmit the specified data from the source node to destination node is plotted in the y-axis. It is observed that as the number of nodes increases, the time taken to transmit data packets is high in the case when the compression technique is not used. With the implementation of SLZW algorithm, it is observed that the time taken to transmit data packets is much less. The SLZW algorithm shows better results compared to MLZW algorithm. Therefore the Fig.4 concludes that by using the SLZW algorithm, the transmission delay can be minimized.

4.2 Effect of Key length variation

We compare the change in Security performance by using different key lengths for proposed algorithm. Graph is plotted between the time required to find the correct key and different key lengths. We have taken six different scenarios by increasing the length of the key.

Table 2: Different Key lengths

Scenario	Key Length
1	8 bit
2	16 bit
3	24 bit
4	32 bit
5	40 bit
6	48 bit

The following graph for scenarios as stated in Table 2. The figure 5 shows that the Number of seconds required to breach the corresponding algorithm against brute force attack.

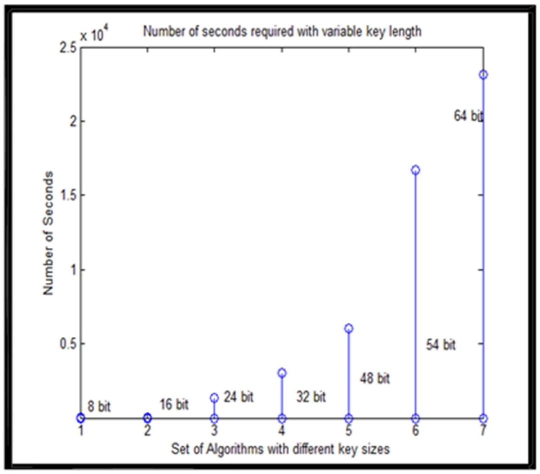

Fig. 5. Brute Force Analysis Test

The above graph shows that the time taken to find a key by the brute force analysis on proposed model for different key lengths. From this graph it is analyzed that time taken by brute force attack increases exponentially with increase in the key length.

5 CONCLUSION & FUTURE WORK

Thus the proposed security scheme with the combination on encryption & compression improves the security of the network and minimizes the memory requirement, bandwidth and power requirement. Using the compression technique and security concept it concludes that any text or document file can be compressed to a maximum of one-third of its original size without any loss of data. From our study we conclude that the proposed security concept may increase the level of confidence in this network and the strength of the SLZW can increase by increasing the number of iteration levels by which the Brute force analysis may take longer time to breach the algorithm.

This work can be extended for implementing:

- Authentication when introduced before the encryption and decryption process will make a more complete security model.
- Power control protocols to reduce the power, which in turn increases the battery life.
- Reduce Network contention
- QoS Topology Control in Ad Hoc
- Wireless Networks

6 REFERENCES

[1] Prasant Mohapatra, Jian Li and Chao Gui, “QoS in Mobile Ad Hoc Networks”, Department of Computer Science, University of California, Davis, CA 95616, National Science Foundation Magazine, December 2002.

[2] Kenneth Barr and Krste Asanovi´c., “Energy Aware Lossless Data Compression”, May 2003.

[3] Dave Marshall, “Lempel-Ziv-Welch Algorithm”, April 2001.

[4] Mark Nelson, “LZW Data Compression”, Dr. Dobb’s Journal, October 1989.

[5] Sooraj Bhat, “LZW Data Compression”, March 2002.

[6] M.Madhurya, B.Ananda Krishna and T.Subhashini “Implementation of Enhanced Security Algorithms in Mobile Ad hoc Networks”, International Journal of Computer Network and Information Security, 2014, 2, 30-37

[7] Wenjing Lou, Wei Liu and Yuguang Fang, “SPREAD: Enhancing Data Confidentiality in Mobile Ad Hoc Networks”, IEEE Conference on Computer Communications (INFOCOM 2004), Hong Kong, China, March 2004

[8] R. A. Vasudevan and S. Sanyal. “A Novel Multipath Approach to Security in Mobile Ad Hoc Networks (MANETs)” International Conference Computers and Devices for Communication (CODEC’04)

[9] B.Ruxanayasmin, B.Ananda Krishna and T.Subhashini, “Minimization of Power Consumption in Mobile Ad hoc Networks”, International Journal of Computer Network and Information Security, 2014, 2, 38-44

[10] Diaa Salama, Hatem Abdual Kader, and Mohiy Hadhoud, “Studying the effects of Most Common Encryption Algorithms”, International Arab Journal of e- Technology, Vol. 2, No. 1, January 2011.

[11] GloMoSim: Global Mobile Information Systems Simulation Library. http://pcl.cs.ucla.edu/projects/glomosim/