VOL. 11, NO. 2, JANUARY 2016 ISSN 1819-6608
ARPN Journal of Engineering and Applied Sciences


www.arpnjournals.com

ENCRYPT - SECURITY IMPROVED AD HOC ON DEMAND DISTANCE VECTOR ROUTING PROTOCOL (En-SIm AODV)

B. Karthikeyan[1], N. Kanimozhi[2] and S. Hari Ganesh[1]
[1]Department of Computer Application, Bishop Heber College, Tiruchirapalli, Tamil Nadu, India
[2]Department of Computer Science, Shrimati Indira Gandhi College, Tiruchirapalli, Tamil Nadu, India
E-Mail: bkarthikeyanms@yahoo.com

ABSTRACT

Resent days Mobile Ad Hoc Network (MANET) mostly uses reactive on-demand routing protocols where routes are launch only when the node needed. Most of the protocols which one is belongs to this category are not including proper security facilities. A MANET is a collection of autonomous mobile nodes with self-configuring, self-administrating features. The Mobile ad hoc environment is accessible by both genuine network users and malicious network attackers. Packets that are routed during route discovery itself it has to be protected in such a way that it has minimum chance of having a malicious node in path formed. In this paper the proposed En-SIm AODV (Encrypt-Security Improved Ad Hoc on Demand Distance Vector Routing Protocol) is the upgraded version of the SIm AODV (Security Improved Ad Hoc on Demand Distance Vector Routing Protocol) which one comes from the previous work. The proposed work uses the private key encryption and decryption to avoid intrusions.

Keywords: self-configuring, En-SIM AODV, SIm AODV.

INTRODUCTION

Security is the major concern in network like MANET where any node without any authentication comes in the network and leaves network. In MANET there is no central authority that can govern the authentication of nodes, which can make sure that the nodes in the network are not malicious.

Mobile Ad hoc Network: Attacks

These attacks are divided 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. An attacker just secretly listen the network traffic as to determine which nodes are trying to establish routes, or which nodes are important 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 downward the network. The attitude of attacks varies greatly from one set of circumstances to another. Some of the generic types of attack that might be encountered in passive attacks are:

Interruption: An asset of the system is ruined, becomes unreachable. This is an attack on availability. Examples include destruction of a part of hardware, or cutting from a communication line.

Interception: An unauthorized party gains access to resources. This is an attack on secret manner. The unauthorized party could be a individual, a program or a system. Examples include wiretapping to capture data in a network or the illicit copying of files.

Modification: An unauthorized party tampers with an resource. This is an attack on honesty. Examples include altering 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 fake messages in a network or the addition of records to a file.

Active Attacks

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

Replacement: In this attack one object pretends to be a different object. It is done by someone familiar with your security procedures and failures. An impersonate attack usually includes one of the other forms of active attacks.

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

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 in-between, listening in on your communications and possibly modifying them.

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 inactivating the network or by over heading it with messages so as to degrade the performance. It is like

shutting down a server that could not otherwise be compromised.

Intrusion Detection Schemes

MANETs present a number of unique problems for Intrusion Detection Systems (IDS). Differentiating between malicious network activity and fake, but typical, problems associated with a mobile ad hoc networking environment is a challenging task. In a mobile 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 perform maliciously only at regular intervals, further complicating their detection. The loss or capture of unattended radios and personal computing devices may allow for a malicious node to obtain legitimate credentials and launch more serious attacks. A node that sends out fake routing information could be a compromised node, or simply a node that has a temporarily stale routing table due to volatile physical conditions. Constant changes in topology make it difficult to obtain a global view of the network and any approximation can become quickly invalid. Traffic monitoring in infrastructure wired networks is usually performed in network device (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 doubtful nodes. A MANET is most likely not under a single administrative domain, making it hard to perform any kind of centralized management or control.

RELATED WORK

Sunil Taneja *et al*: Key management is the process by which cryptographic keys are manipulated (generated, stored, protected, transferred, loaded, used, and destroyed). The data packet will be transmitted from source to destination over transmission media using efficient cryptographic algorithm to encrypt the entire packet.

Rajdeep S. Shaktawat *et al*: This author's algorithm uses a fully distributed authority approach in which every node in network has its own itself certifying authority. Whenever a node enters into the network during its boot time it will generate two set of public and private key and make a communication.

A. Jegatheesan *et al*: This scheme shares the key between source and destination which is more resistant against internal and external attacks. The design of our scheme offers strong privacy protection – complete unobservability, unlinkability and anonymity – for ad hoc networks.

Tagare Rachana *et al:* The sensor network is splitting into clusters with cluster head for each cluster. We assume that each sensor node has a unique ID The cluster leader or cluster head knows the IDs of its sensor node in its cluster. The nodes in its cluster transmit the information or data to the cluster leader or cluster head in place of sending data immediately to the sink or destination node.

K. S. Abitha *et al*: according to this work it increases security considerations of the network using AODV algorithm for transfer of data and to increment the efficiency of AODV algorithm using ECC (Elliptic Curve Cryptography). Reliability and Efficiency will be increased in each transmission, while enclosing the proposed method by using the ECC algorithm which allow itself to encrypt and decrypt the data that is to be transferred and performs the active classification.

S. Abila Judith Suganthi *et al*: The more nodes cooperate to transfer traffic, the more powerful a MANET gets. Detecting routes and forwarding packets consumes network bandwidth, local CPU time, memory, and least energy. In this work, author found the dropping packets for optimal estimation by using path tracing algorithm in reputed AODV.

PREVIOUS WORK

SIm AODV routing protocol gives excellent packet delivery ratio around 97%. Still this algorithm does not have any encryption technique to provide the security. In this SIm AODV has around five different algorithms, to prevent the packet loss from Black Hole Attack, Cosmic Dust Attack, Link Break, and Node Intrusion by the malicious and unbelievable nodes. But the end-to-end time taken is very poor compare to the normal AODV. At present what the SIm AODV has is enough to prevent the packet loss. But this is not enough for the future MANET. Because, the future network will become more dense and more big in size. So prevention of packet loss is not only enough, it needs security on data theft as well as more speed.

This proposed work En-SIm AODV(Encrypt-Security Improved Ad Hoc on Demand Distance Vector Routing Protocol) is the cover of the SIm AODV. It concentrates only on encryption of data to make secure communication from the source to destination with minimum packet loss (which one given by SIm AODV).

PROBLEM STATEMENT

The SIm AODV has the capable to prevent packet loss owed by Black Hole Attack, Cosmic Dust Attack , Link Break, and Node Intrusion by the malicious and un believable nodes.

But SIm AODV has two major problems one is it does not has the mechanism to prevent active attacks. Second one is end-to-end delay is more compare to the normal AODV.

The proposed En-SIm AODV overcomes the data change or theft by the malicious node. This En-SIm AODV algorithm uses PrKeyP (Private Key – Parity Bit) algorithm for key based encryption and decryption and parity bit check.

Initially the data is split into 7 bits words. Each and every 7 bits word's parity bit will be calculated and

this parity bit is added in the 7th location of the word. It became 8 bit or 1 byte word.
Data 01101011110110
Data after split by 7 bit word
Data 0110101 1110110
0110101 parity bit is 0 its added as 7th bit so 00110101
------- First Word
1110110 parity bit is 1 its added as 7th bit so 11110110
------- Second Word

The Encryption and Decryption Key is one of the private key. It's size is 16bits or 2 byte. It will be communicated during the Path Discovery time. This Private Key is make XNOR operation with the data and it gets the chipper text this text is transmit to the destination
Encryption and Decryption Key is
'61 53'
Word Location

	First	Second
Bits Location	7654 3210	7654 3210

Encryption and Decryption Key is
'1011 1101 1101 0111'
6 1 5 3

When the packet reaches the destination, destination again Decrypt by the use of Encryption and Decryption Key which one is communicated during the Path Discovery. The received chipper text again XNOR with the key and the receiving end will get the plain text.

The plain text has to split into 8 bits words, and calculate the parity bit using 0th position bit to 6th position bit and compare the calculated parity bit with the 7th position bit if it is equal there is no data loss. This is the data which one the source wants to communicate with the destination.

PrKeyP Encryption Algorithm

Step 1: Split available data into 7 bits word
Step 2: Calculate parity bit with 7bit data
Step 3: Add Parity bit into 7th location (8th) bit of the 7bit word
Step 4: Group every 2 byte data
Step 5: 2 byte data XNOR 2 byte Private Key
Step 6: Process for Transmission.

Flow Diagram for PrKeyP Encryption Algorithm

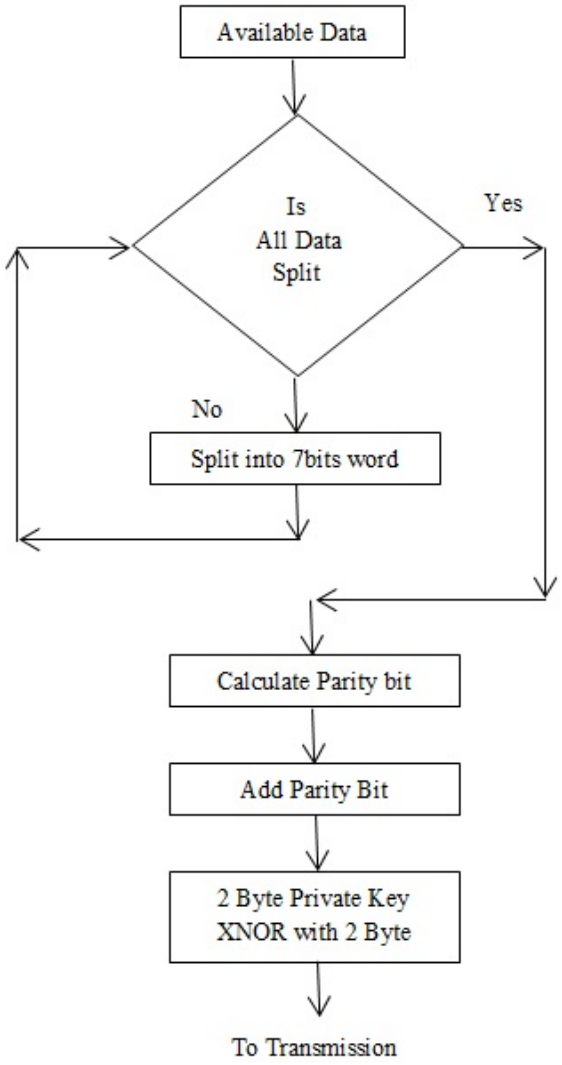

Figure-1. Flow chart for PrKeyP encryption.

PrKeyP Decryption Algorithm

Step 1: Process for Receiving. Split available data into 7 bits word
Step 2: Group every 2 byte Chipper text.
Step 3: 2 byte Chipper text XNOR 2 byte Private Key.
Step 4: Group every 8 bit data.
Step 5: Calculate parity bit with 7bit data.
Step 6: Compare Parity bit with 8th position bit in the 8 bit data. If true go to Step 8
Step 7: Request Retransmission.
Step 8: Data which one the source wants to communicate with the destination.

Flow Diagram for PrKeyP Decryption Algorithm

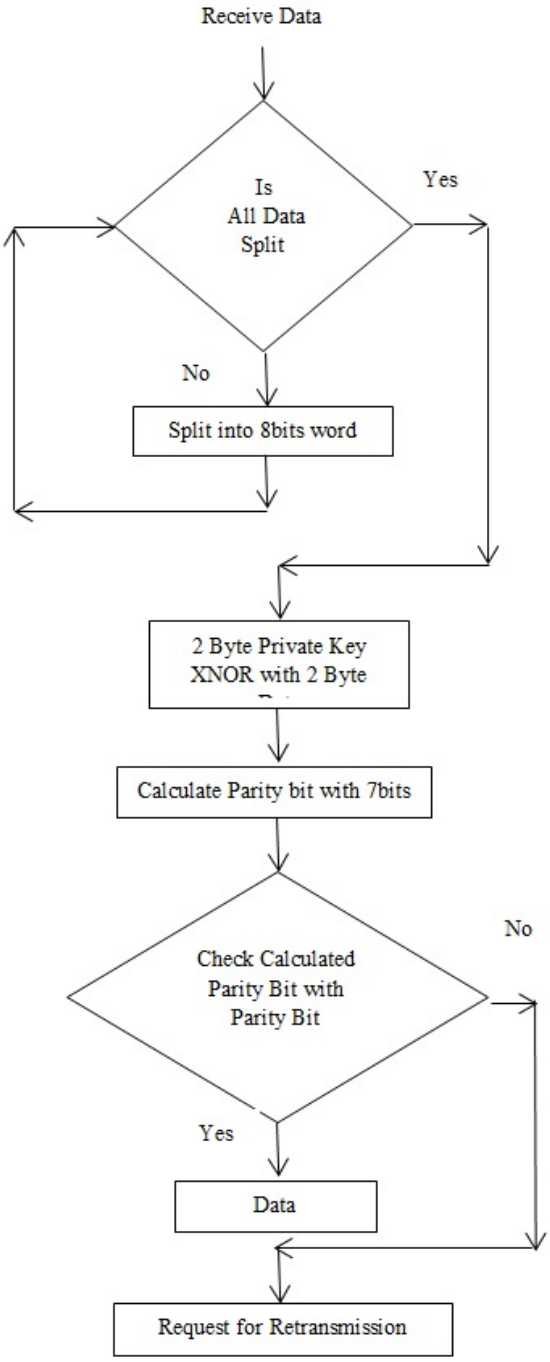

Figure-2. Flow chart for PrKeyP decryption.

METHODOLOGY

In order to analyze the performance of the AODV routing protocols, with respect to the following metric:

Throughput or packet delivery ratio: It is calculated by the numbers of packets sent out by the sender application and the number of packets correctly received by the corresponding peer application.

Average end-to-end delay: This implies the delay a packet suffers between leaving the sender application and arriving at the receiver application.

a) Simulation

OMNeT++ is an object oriented discrete event simulation environment developed by Andr´as Varga at the Technical University of Budapest. Its major use is in simulation of network communications. The developers of OMNeT++ predict that one might use it as well for simulation of compound IT systems, queuing networks or h/w architectures, since OMNeT++ is built generic, more flexible and modular. As the architecture is modular, the simulation kernel and models can be embedded easily into an application. C++ programming structure is used for the modules in OMNeT++.

b) Simulation Parameters

Table-1. Simulation parameters.

Parameters	Values
Network Size	600m X 600m
Number of Nodes	0-50
Max. Speed/Mobility	10.0ms/s
Pause Time	0-100s
Traffic Model	CBR
Routing Protocol	AODV UU with SIm AODV , En-SIm AODV
Simulation Time	600s

RESULT AND DISCUSSION

Table-2. Throughput vs number of nodes.

Number of Nodes	AODV (PPs)	SIm AODV (PPs)	En-SIm AODV (PPs)
10	18	25	24
20	40	42	40
30	60	83	78
40	96	109	102
50	121	145	130

Note:- PPs – Packets Per Second

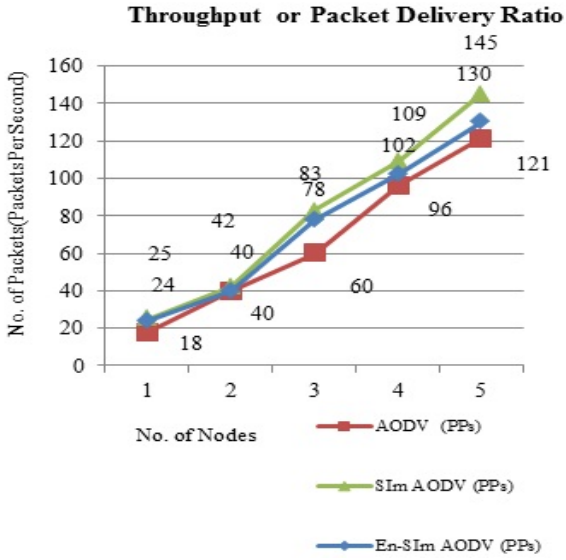

Figure-3. Throughput vs no. of nodes.

Table-3. End-to-end delay vs. number of nodes.

Number of Nodes	AODV*(ms)*	SIm AODV*(ms)*	En-SIm AODV*(ms)*
10	3.11	4.88	3.72
20	4	5	4.26
30	4.55	7.4	6.12
40	6.63	8.82	7.26
50	5.9	11	9.5

Figure-4. End to end delay vs. no of nodes.

CONCLUSIONS AND FUTURE WORK

En-SIm AODV algorithm decreases the packet loss and increase the security based on private key encryption. But this is has the great problem in end to end (transit) time taken for deliver the packet. Compare to the SIm AODV En-SIm AODV is provide average throughput with more security. It took less transit time compare to SIm AODV, and more transit time compare to AODV. The En-SIm AODV more than good in packet delivery ratio and packet security. En-SIm AODV has moderate problem with time taken to reach the destination. It has to overcome in the future that means the transit time have to reduce.

REFERENCES

[1] B. Karthikeyan, N. Kanimozhi and Dr. S. Hari Ganesh, Performance and Analysis of Ad-Hoc Network Routing Protocols in MANET,NCAC, April 2013, pp 65-71.

[2] B. Karthikeyan, N. Kanimozhi and Dr. S. Hari Ganesh, "Analysis of Reactive AODV Routing Protocol for MANET"‖, IEEE Xplore, Oct 2014, pp 264-267.

[3] B. Karthikeyan, N. Kanimozhi and Dr. S. Hari Ganesh, "Complexity in Security Issues of MANET Pertaining to AODV Protocol", International Conference on Contemporary Trends in Computer Science (CTCS - 2014). Feb 2014, pp. 264-267.

[4] B. Karthikeyan, N. Kanimozhi and Dr. S.Hari Ganesh, "Security and Time Complexity in AODV Routing Protocol", IJAER, pp15542- 155546, Vol. 20,June 2015.

[5] Sunil Taneja, Sima Singh, Ashwani Kush," Encryption Scheme for Secure Routing in Ad Hoc Networks", IJICT, Vol. 1, No. 1, ISSN 0976-4860,2011,PP 22-29.

[6] Rajdeep S. Shaktawat, Dharm Singh, Naveen Choudhary, "An Efficient Secure Routing Protocol in MANET Security - Enhanced AODV (SE-AODV)",IJCA (0975 – 8887), PP 34-41. Volume 97– No.8, July 2014.

[7] A. Jegatheesan, D. Manimegalai," Secure Key Sharing in Mobile Ad hoc Network using Content Invisibility Scheme", WSEAS transactions on computers, E-ISSN: 2224-2872, Volume 14, 2015,PP 124-133.

[8] Tagare Rachana, Upasana Patil, Deepak Biradar, " A Novel Approach for Secure Data Transmission and Clustering based Energy Efficient in Wireless Sensor Networks", International Journal of Computer Application (2250-1797) Vol. 5, No. 4, June2015,PP152-159.

[9] K. S. Abitha, Anjalipandey, Dr. K. P. Kaliyamurthie," Secured Data Transmission Using Elliptic Curve Cryptography", International Journal of Innovative Research in Computer and Communication Engineering, Vol. 3, No. 3, March 2015,PP 1419-1425.

[10] S. Abila Judith Suganthi, P. Rajesh, "Encryption Based Intrusion Detection in MANET using Aodv Routing Protocol", Elysium Journal, P-ISSN: 2347-4408, Volume - 2, Issue – 2, April 2015.