QALAAI ZANIST JOURNAL

A Scientific Quarterly Refereed Journal Issued by Lebanese French University – Erbil – Kurdistan – Iraq

Vol. (2), No. (2), April 2017

Speical Issue : The 1st International Conference on Information Technology (ICoIT'17)

ISSN 2518-6566 (Online) - ISSN 2518-6558 (Print)

Survey and New Security methodology of Routing Protocol in AD-Hoc Network

Shahab Wahhab Kareem

Department of Information System Engineering, Technical Engineering College, Erbil Polytechnic University - Erbil, Kurdistan Region, Iraq
shahabwk@yahoo.com

Dr.Yahya Tareq Hussein

Department of Information Technology, Lebanese French University - Kurdistan Region, Iraq
Dr.yahya@lfu.edu.krd.

ARTICLE INFO

Article History:

Received: 17 March 2017

Accepted: 1 April 2017

Published: 10 April 2017

DOI:

10.25212/lfu.qzj.2.2.43

Keywords: *wireless sensor network (WSN); Multipath routing protocol; WLAN; Minimum Spanning Tree; Mobile Ad hoc network.*

ABSTRACT

Because of many reasons routing is the complex task in ad hoc sensor network. The self-organizing network which is Mobile ad hoc network (MANET) its established automatically via wireless connections by a combination of portable nodes without the support of a centralized management or static infrastructure. The portable nodes redirect packets among these nodes, enabling connection between nodes outside the range of wireless transmission hop by hop capabilities are necessary. So it important is increasing to provide suitable routing protocol plus security. This paper endeavors to present a full survey about secure routing. At the beginning investigates the reason which makes ad hoc network is susceptible to attacks. After that, it shows the well-known traditional secure protocols then compares them. Finally, the proposed algorithm depended on the Dynamic Source Routing (DSR) to remove malicious nodes, minimum spanning tree for routing path plus coding-encryption technique of a chaos-based adaptive arithmetic for encrypting, compression plus decompression, decrypt a message.

1. INTRODUCTION

In every wireless networking environments in today's abundant use of communication devices, nodes communicate by two methods either shortly with their planned communication partner or in the form of base stations which is called networking infrastructure as well as a backbone network. Example, the using 802.11 in ad hoc networks, shows the components also the networks inside the Wireless Network Infrastructure. The self-organizing network which is Mobile ad hoc network (MANET) its established automatically via wireless connections by a combination of portable nodes without the support of a centralized management or static infrastructure. In the portable ad hoc networks

every nodes provided by a receiver plus transmitter. This wireless receiver and transmitter enable the nodes at the same radio communication range to contact with each other. Habitually nodes participate with the same physical media; they transmit and collect signals at the same frequency band, and follow the same step sequence or broadcasting code [1].
An attacker may produce malicious nodes that forward only certain messages and drop others. In order to grab the route forcibly, a Black Hole attack can execute via only one node which counterfeits the hops count and sequence number of a routing message. Then the Black Hole node will snoop, or immediately discard the received data packets. The type of Denial Services attack is a Gray Hole. Here the node forms wrong routing information in the network. A Gray Hole discard just a part of the packets do not drop all the packets [2]. In the proposed algorithm the malicious removed (black hole and gray hole) by using DSR routing protocol in the Ad hoc network. After removing all malicious by using the minimum spanning tree to select the shortest path routing protocol for sending and receiving a message, finally Using Chaotic System and Variable Model Arithmetic Coding to make Compression and Encryption Scheme.
This paper contains: Section 2 describes some algorithms for routing protocol, section 3 comparison between algorithms and designing proposed, in section 4 plan of work is discuss, in section 5 the conclusion.

2. SECURE ROUTING

Protected routing protocols overcome malevolent nodes that be able to obstruct the accurate operation of a routing protocol by adjusting routing information, via imitating other nodes and by inventing false routing information. This Protected routing protocols of ad hoc networks are either combinations of security mechanisms within the existing protocols or entirely novel independently protocols. In general, the proposed secure routing protocols was classified into two classes, routing protocols which use hash chains and routing protocols that require predefined dependence relationships in order to operate [1].

- hash chains is A one-way hash function H(.)to be more secure in routing protocol is to follow these properties:
  1-H(.) can take a message of arbitrary length as input and produce a message digest of a fixed-length output.
  2- Given x, it is hard to compute $H-1$ (y) = x given y. However, it is easy to compute H(x) = y.
  3- Given x, its arithmetically not practicable to determine x'≠ x such that H(x') = H(x) [3].
- Basic of Chaotic Systems Properties it's designed via few simple function f which is repeated on some set X. Especially, the mapping f: X→X is said to be chaotic on X if
  - Periodic points are thick in X.

- f is topologically transitive;
- f has sensitive reliance on initial conditions;

In intuitive way, a map owns sensitive reliance on primary situations if there exist points arbitrarily near to x which finally separate from by at least δ > 0 under repetition of f, while a topologically transitive map has points that ultimately transfer in repetition from one random minor neighborhood to any other [4].

In this paper, we presented a survey for secure routing and proposed secure routing based on Paillier public key for encrypt and decrypt the Message and also used DSR to remove these malicious nodes, and minimum span tree for routing path are used. The following are some of the routing protocol discussed.

- Methodology for Securing Multipath Routing
- The Ad-Hoc Demand Distance Vector(AODV)
- A Simulation Study of Security Performance Using Multipath Routing in Ad Hoc Networks DSR.
- A Novel Method of Secure Routing Protocol: for Improve Network Life.

2.1. THE AD-HOC DEMAND DISTANCE VECTOR (AODV)

This algorithm also can be called a pure on-demand route acquisition system; Nodes does not give false data to active paths either share or exchange information about the routing table nor keep this information. Additional, a node does not have to maintain and discover a route to another node until the communicate between two nodes needed, the fig-1- below shown the routing discover process unless the former node which is an intermediate routing station provides its services to maintain communication between two other nodes[5].

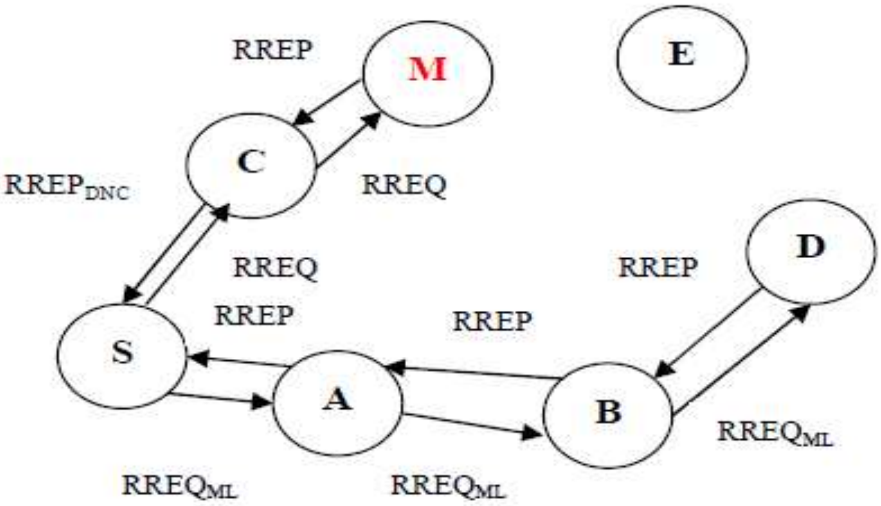

FIGURE 1. Route discovery process of AODV

The importance connectivity of the local mobile node makes each mobile node uses multiple techniques to become more aware of neighboring nodes, one of these technique includes local broadcasts known as hello messages (not system-wide). The routing tables are designed to optimize response time of the nodes within the neighborhood to local movements, and due to the requests of new routes, this technique provides fast response time. The primary objectives of the algorithm are:

- Discovery packets were broadcasting when it needed only.
- To differentiate between management of local connectivity and maintenance of general topology.
- To distribute information to mobile nodes that needs the information about changes in local connectivity.

2.2. MEHODOLOGY OF SECURING MULTIPATH ROUTING

A protocol is responsible for the protection which implemented by using a digital signature, this digital signature generated by applying the encryption algorithm and MD5 hash function [2]. The correctness of data, nonrepudiation, and authentication is security ensures. The protocol supports Byzantine attacks; sink hole, selective forwarding and data tampered or altered routing. Ad hoc On-demand Multipath Distance Vector (AOMDV) routing protocol is regularly applied in Wireless Sensor Network [6].

In AOMDV, the network is inactive while waiting for a fresh connection is required. When any node requires communicating with others, it transmits a request for connection. Another AOMDV nodes for a second time transmits this message, then keep the nodes log that they received from; each node remains this process till target node get [7].

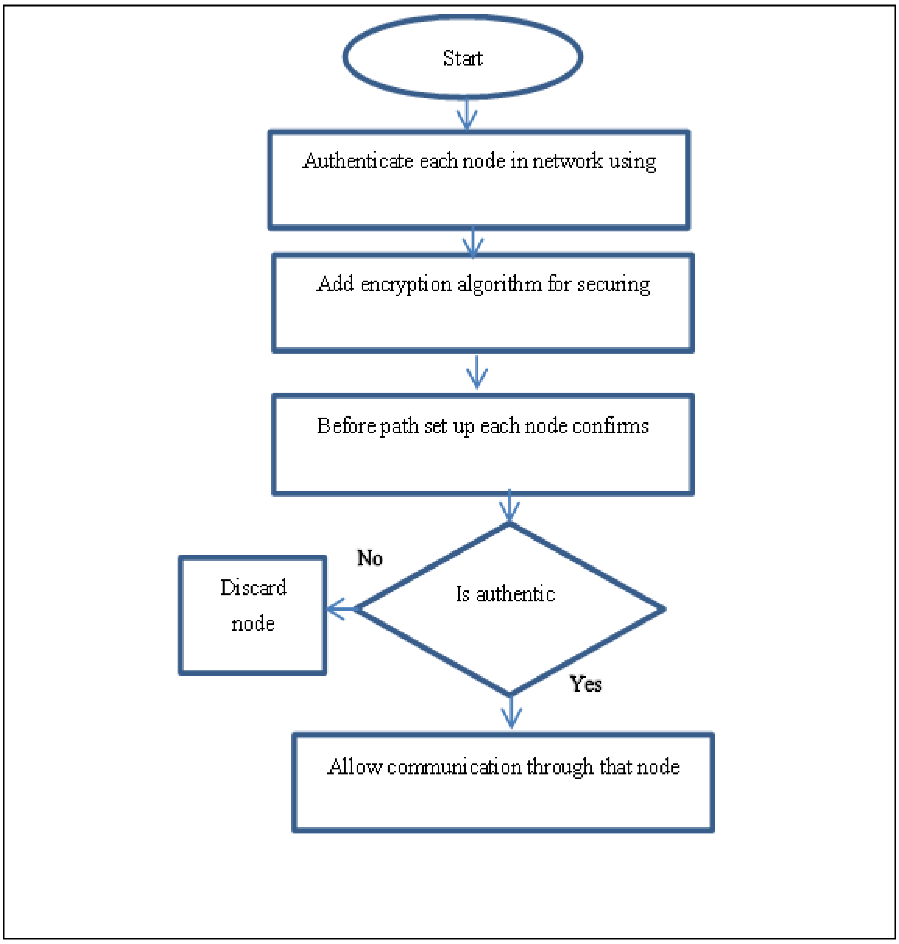
Start
Authenticate each node in network using
Add encryption algorithm for securing
Before path set up each node confirms
No
Discard node
Is authentic
Yes
Allow communication through that node

FIGURE 2. Flow Diagram of Multipath Routing

The figure 2 has shown the process flow diagram of the algorithm [8]. Nodes transmit messages back over a momentary route to the requesting nodes which are desire to send message to the wanted node after receiving this message. The node chooses the shortest route for communication that which begins the process (i.e. just the route that having the minimum number of hop count). Determined the behavior plus characteristic of the attack from several parameters. Broadcasting messages are to maintain the capacity of the wireless network. A rapid substantiation is complete to assess and confirm the dubious attack [9].

2.3. A Novel Method to Improve Life of Network for Secure Routing Protocol

The procedure for of working start in login to account (for new user create an account) after this authenticate it by username, password and secret question to authorize. Then generate path step and choosing file /data to encrypt file/data by using Advanced Encryption Standard (AES) algorithm and send it to the desired node through selected path. At the destination node, the user verifies whether the received data for reliable/pure or malicious if data after verification goes to reliable the data is pure otherwise, data is not pure (The intruder is attacking data). Recognize the attack data and reject it and finally negative acknowledgment sent to the source [10]. The following pseudo code of the algorithm:

```
1. Start and login process
2. if register then login and authenticate and authorized
3. Else create a count and repeat step 2.
4. generate secure path.
5. send file (encrypted file) at source and receive file (decrypt
   file) at destination
6. verifies data (if pure data ) its save it
7. Else identify the node that send data by vampire attack.
8. reject data and send negative acknowledgement to the source.
```

2.4. A Simulation Study of Security Performance

The SPREAD scheme reduce the message interruption which is the result of eavesdropping or compromising nodes by combines a multipath routing and secret sharing [11]. The secret message is dividing to several (N) parts (called shares). This dividing is by utilizing a threshold secret sharing scheme (T, N), it can simply retrieve the message so that from every T or more shares. It is impossible to retrieve the message while from any shares (T-1) or less. By applying link encryption for this scenario where SPREAD is implemented. To negotiate between the two neighboring nodes, each link uses a dissimilar encryption key (e.g. using the Diffie-Hellman key exchange protocol). For composition the messages, the opponent can either overhear the sending and receiving of all network then trying brute-force decryption or compromise the nodes these interrupt all the secrets transmitted [11].

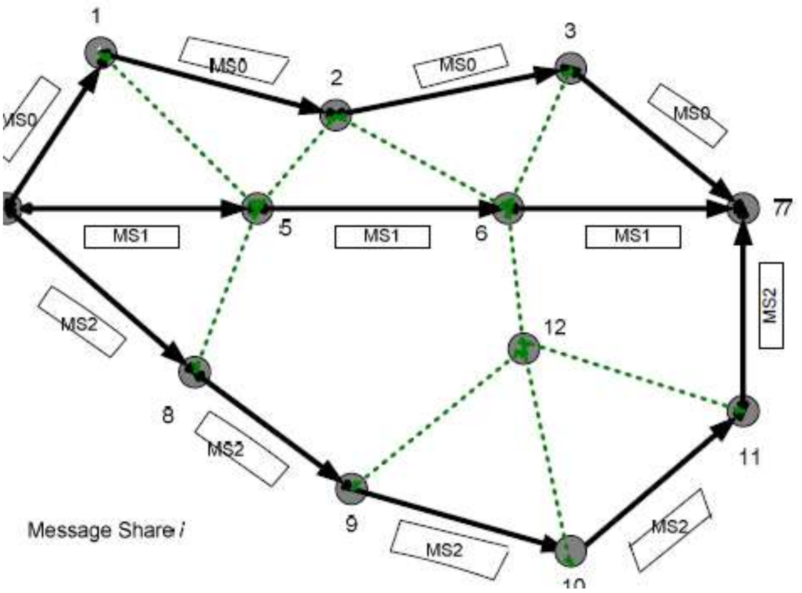

FIGURE 3. Illustration of multipath routing

From network viewpoint, an opponent may interrupt all the essential information, if all message follows a single route to its destination, to retrieve that message with compromising any node on the route [11]. With the SPREAD scheme, excepting the destination and source nodes, the opponent should conciliation some nodes inside network on a number of independent routs to find the least required (T) shares. Considering the multipath routing and the scenario of (3, 3) secret sharing as shown in Figure3.

2.5. Dynamic Source Routing (DSR)

DSR is an on-demand protocol designed to limit the bandwidth occupied by control packets in ad hoc wireless networks by dropping the periodic table update messages which required in the proactive routing protocols. In the network, to connect node with another node, initially, need to discover a proper path in order to follow while transmitting packets to the destination node. While the requirements stay without change, this path should then continue to work for as long as it is needed. For the benefit of the intermediate nodes, in this protocol every potential information extracted from the source path and stored within route cache that contained in a data packet. DSR also allows piggy-backing of a data packet [12].

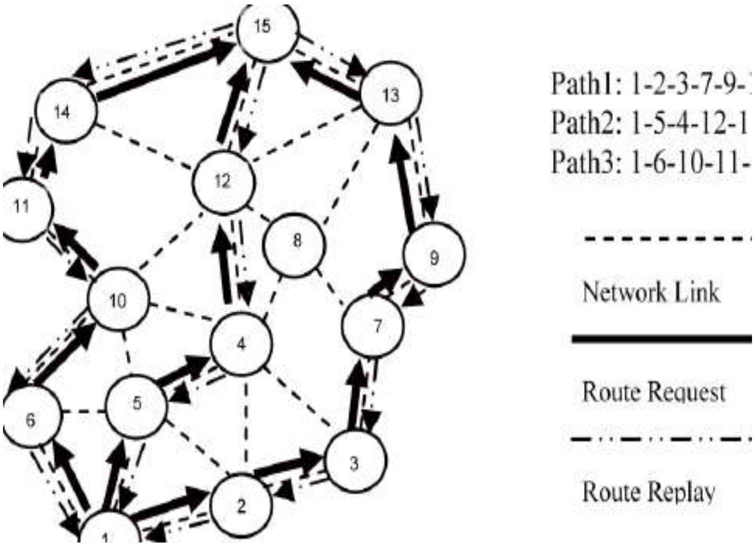

FIGURE 4. Route establishment in DSR.

In the Maintenance procedure when an intermediate node in the network is moving away or drop making a break in the wireless link, an error message is created from the node adjacent to the broken link to inform the source node in a whole network. The source node reinitiates establishment procedure for the route. When a Route Error packet is received the source node is removed and the cached entries at the intermediate nodes. Figure 4 illustrates the working of DSR [12].

3. Comparison Between The Algorithms

The following shown the comparison in table 1 depended on similar type routing protocol, routing protocol, advantage and disadvantages of the above algorithms [1][2][3][4][13][14][15][16][17][18].

TABLE 1: comparison types of routing protocol

Name	**Type Routing protocol**	**Routing protocols**	**Techniques**	**advantage**	**Disadvantage**
AODV	REACTIVE	capable of both unicast and multicast routing with loop free routes	Gets single path from the available funded path, and the source sends all its packet through this one funded path.	reduce the control traffic message overhead.	increase latency in finding new routes.

AOMDV	REACTIVE	multicast routing	Gets multipath from the route funded path between each source and destination	allows the intermediate nodes to reply to RREQs.	increased flooding.
Novel Approach	REACTIVE	broadcasting	Each node starts as its own group of size one, with a virtual address 0. Nodes broadcasts form groups with their neighbors	not depend on any protocol, design properties.	exploit simple properties of protocol like distance vector.
SPREAD	REACTIVE	combines the secret sharing and multipath routing	Divide the secret message into N parts that used to find multi secure path.	aggregating bandwidth, reducing blocking probability.	Severe collisions at MAC layer.
DSR	PROACTIVE	broadcast	Divided into two types routing discover and routing maintenance	Route maintenance mechanism	the link is broken or a change is noticed another path is chosen

4. Methodology Of Proposed Study

The mechanism of an efficient security is established to protect the communication inside the network (connection between nodes) and to prevent attacks of Black hole and Gray hole by using DSR. In this mechanism, when several nodes configured the network is from this network are examined and checks whether there are malicious nodes to remove by using the use of advanced DSR protocol mechanism.

Then a spanning tree creates to calculate the least distance between every/each node which can cover network without making a cycle. Then we select the route with minimum distance. For security and compression we use the ciphers based on chaotic systems and arithmetic coding, which uses the secret information (the key which Based on the initial condition/parameters for the chaotic map). The system proposal is shown in Figure 5.

4.1. A-DSR Routing Protocol

In the development method, the stirrer is transmit a Route Request packet, recognizing the destination to which the route is required. In general, any node upon receiving the Route Request, in case that if it has not already forwarded a copy of the Route Request it will retransmits the request; when the request received by target node the, a Route Reply backward to the stirrer, rather than forwarding the request, listing the route taken by the Request. Route reply for each copy of the route request that it receives will return by target node; "Each Route Request packet carries a sequence number generated by the source node and the path it has traversed. A node upon receiving the Route Request packet, checks the sequence number on the packet before forwarding it. The sequence number on the packet is used to prevent loop formations and to avoid multiple transmissions of the same Route Request packet by an intermediate node that receives it through multiple paths" [12].

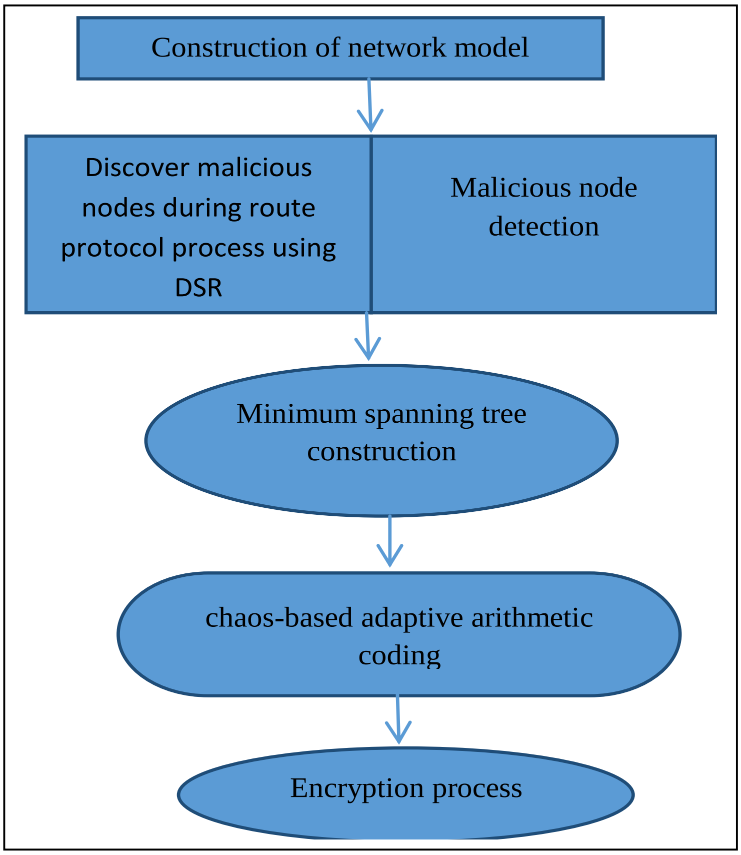
Construction of network model
Discover malicious nodes during route protocol process using DSR
Malicious node detection
Minimum spanning tree construction
chaos-based adaptive arithmetic coding
Encryption process

FIGURE 5. Proposed System Architecture

4.2. Spanning tree construction

The minimum distance of spanning tree is calculating between every / each nodes which can cover all the nodes without forming a cycle. Spanning tree holds security tie-ups only with neighbor. Spanning Tree Protocol is a network protocol which maintains plus establishes this network by connecting a group of portable node in the wireless ad hoc network. the process of calculating minimum span tree shown in Figure 6 [14].

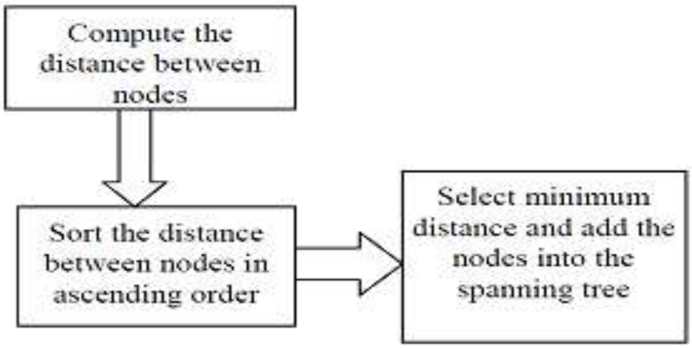
Compute the distance between nodes
Sort the distance between nodes in ascending order
Select minimum distance and add the nodes into the spanning tree

FIGURE 6. Construction of spanning tree

4.3. Security and Compression Mechanism

Chaotic and arithmetic coding mechanism is used to ensure security. Each and every node from the mobile ad-hoc network has its own system. The model that execute zeroth-order adaptive arithmetic coding. Figure 7 shows that the encoder block that uses the secured information that depends on the modified arithmetic coder (this key is based on the first condition/parameters for the chaotic map) this secured information is to coding the initial file for the plaintext, so, the output will be encrypted and compressed. The insecure channel that transmit the data that are coded to the encoder block will be secured by the information that resulted from the encoder block, while the key for the chaotic map will transferred by a private, secure channel. Figure 7 shows the process for encode, encrypt and decode and decrypt message from sender to receiver.

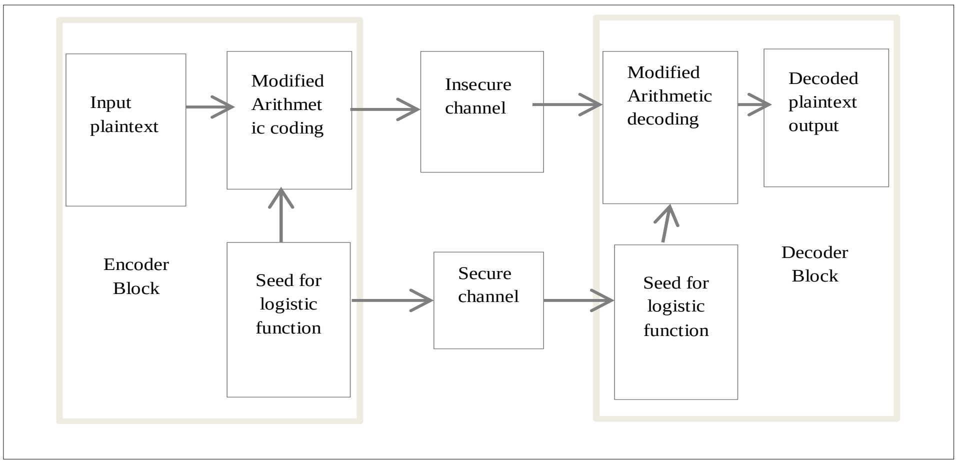
Input plaintext
Modified Arithmet ic coding
Insecure channel
Modified Arithmetic decoding
Decoded plaintext output
Encoder Block
Seed for logistic function
Secure channel
Seed for logistic function
Decoder Block

FIGURE 7. Chaotic and arithmetic coding

5. CONCLUSION

Mobile Ad hoc Network requires the high level of security as compare to the regular wired networks Security issues which is neglected while designing routing protocols for ad-hoc networks. Through DSR protocol, it is easier to infract the security of wireless ad-hoc network. DSR protocol is susceptible to various attacks including Black hole and Gray hole attacks. Efficiently finds short and secure route to the destination. A secure ad hoc network has to meet different security requirements. First privacy concerns require Confidentiality in the use of data. Second Encryption and Decryption by using chaotic cryptosystem is one of the mechanisms used to enforce confidentiality. Third the integrity of data (cipher text) arise to destination must not be modified by maliciously only the authorized user can be decrypted and recover the original data. Fourth the data compression is also an issue for several reasons in Authentication and Non-repudiation refer to the inability to deny the performance of some action falsely. The DSR scheme is depends on the idea to distribute a secret through multiple independent paths while it is transmitted across the network.

6. REFERENCES

[1] Dongbin Wang, Mingzeng Hu and Hui Zhi, “A survey of secure routing in ad hoc networks”, The Ninth International Conference on Web-Age Information Management, © 2008 IEEE.

[2] S. Marti, T. J. Giuli, K. Lai and M. Baker, "Mitigating Routing Misbehaviour in Mobile Ad Hoc Networks", Mobile Computing and Networking. (2000), pp., 255-265.

[3] Yipin Sun, Rongxing Lu, Xiaodong Lin, Jinshu Su and Xuemin (Sherman) Shen, “NEHCM: A Novel and Efficient Hash-chain based Certificate Management Scheme for Vehicular Communications”.

[4] F. Bevitelli, E. Di Cola, L. Fortuna and F. Itnlia, “Multilayer Chaotic Encryption for Secure Communications in Packet Switching Networks” , Communication Technology Proceedings, 2000. WCC - ICCT 2000. International Conference on 21-25 Aug. 2000

[5] CHARLES E. PERKINS, ELIZABETH M. ROYER, “AD-HOC ON-DEMAND DISTANCE VECTOR ROUTING”, MOBILE COMPUTING SYSTEMS AND APPLICATIONS, 1999. PROCEEDINGS. WMCSA '99. SECOND IEEE WORKSHOP.

[6] Parul suneja , Anil Kumar and Annu Soni , “System scenario based investigation of AODV and AOMDV Routing Protocol in MANET” , 2015 International Conference on Soft Computing Techniques and Implementations- (ICSCTI).

[7] Sunita Gupta and Ghanshyam Prasad “Enhanced load balancing and delay constraint AOMDV routing in MANET”, 2016 Symposium on Colossal Data Analysis and Networking (CDAN).

[8] Sukiswo and Muhamad Rifqi Rifquddin ,“Performance of AOMDV Routing Protocol Under Rushing and Flooding Attacks in MANET”, 2015 2nd International Conference on Information Technology, Computer, and Electrical Engineering (ICITACEE)

[9] Vipin Bondreand Sanjay Dorle ‘ “Design and Performance Evaluation of AOMDV Routing Protocol for VANET” , IEEE International Conference on Computer, Communication and Control (IC4-2015).

[10] Sunil Bhutada, ranthi Kumar.K,Manisha.K, “A Novel Approach for Secure Routing Protocol: To Improve Life of Network”, International Conference on Contemporary Computing and Informatics (IC3I), 978-1-4799-6629-5/14 ©2014 IEEE.

[11] Wenjig Lou,Wei Liu,Yuguang Fang, “A Simulation Study of Security Performance Using Multipath Routing in Ad Hoc Networks”, 0-7803-7954-3/03 ©2003 IEEE.

[12] Loay Abusalah,Ashfaq Khokhar,Mohsen Guizani, “A Survey of Secure Mobile Ad Hoc Routing Protocols”, IEEE COMMUNICATIONS SURVEYS & TUTORIALS, VOL. 10, NO. 4, FOURTH QUARTER 2008.

[13] Rabab Mohsin, John Woods, " Performance Evaluation of MANET Routing Protocols in a Maritime Environment" 6th Computer Science and Electronic Engineering Conference (CEEC) university of Essex ,2014.

[14] Sisily Sibichen1, Sreela Sreedhar2 ,"An Efficient AODV Protocol and Encryption Mechanism for Security Issues in Adhoc Networks", (ICMiCR-2013).

[15] Mohsin Ur Rahman and Sohail Abbas "Simulation-based analysis of MANET routing protocols using group mobility model" ,International Conference on Inventive Computation Technologies (ICICT),2016.

[16] Faria Farjana Khan , Anindya Jana , Tahesin Samira and Kazy Noore Alam Siddiquee, "Performance of Agro-Sensors: Assessment of Optimality in Routing Protocols of MANET in Wireless Sensor Networks", International Conference on Intelligent Control Power and Instrumentation (ICICPI) , 2016.

[17] Yue Yang , Siyuan Hao and Haibin Cai , "Comparison and Evaluation of Routing Protocols Based On A Collaborative Simulation Using SUMO and NS3 with TraCI", International Conference on Information System and Artificial Intelligence , 2016.

[18] Guruprasanna and R Sujatha M "A novel Approach to avoid malicious attack to enhance network in WSN", IEEE International Conference On Recent Trends In Electronics Information Communication Technology, 2016.