Analyzed Virtual Routing Protocol for Future Networks (MANET & topological network)

[1]R. Viswanathan, B.E.

CSE Dept. Arulmigu Meenakshi Amman College of Engg
Thiruvannamalai DT, Near Kanchipuram,
vishva.tron@gmail.com

[2]J. Vignesh Kumar, B.Tech

IT Dept, Maamallan Institute of Technology Sriperumpudhur.
vigneshkumarbtech@yahoo.com

[3]T. V. Krishna Prasad, B.Tech

IT Dept. Maamallan Institute of Technology Sriperumpudhur.
krishnait23@yahoo.com

Abstract:

The mobile ad-hoc network (MANET) is a wireless unstructured network and this has mostly suggested for multimedia streaming efficiency. The hackers attacks are reduce the capacity and efficiency of network in MANET. There are various types of protocol are used for the communication in MANET, but security is lacking in those techniques and some insoluble problems present in MANET. In this paper exhibits, a layered protocol network for secured data transmission called Analyzed Virtual Routing Protocol (AVRP). This protocol used to provide more secured data transmission and this not disturbing data streaming in the network.

Keywords:

MANET, Onion Routing Protocol (TOR), **MALBACO,** Internal Attack, Hacking, Encryption, Decryption, Multiplication, Reversible,

1. INTRODUCTION

The Network is defined as interconnection between the users and systems via Internet. With this help of network, we can communicate and transfers the data. Now a day's network is a part of our life. The network is a tool used to communicate one another. This network has to make a connection between two computers from any place, any time. In this network has can be classified into two types, they are topological network and wireless network. In Topological network has to make a data transaction by the help of TCP/IP protocols. TCP means transmission control protocol and IP means internet protocols. These protocols are used to control the data from the source to destination. The wireless network has used some other protocols such as DSR, DSDV, AODV, ZRP protocol for data transmission.

Network topologies may be physical or logical. Physical topology refers to the physical design of a network including the devices, location and cable installation.

In addition, we are using various optional networks in different methods like LAN, MAN, WAN, PAN connections to communicate through internet. But still we are facing these types of problems,

DOI : 10.5121/ijdps.2012.3407

1. Signal.
2. Bandwidth.
3. Speed.
4. Hacking.
5. Security.
6. Redundancy and Durability.

In this connection, we are facing the problem on the topological network like Hacking, threads, collusion and various problems. To destroy that type of problem in many cases. All the problems are almost recovered in this paper by using one new routing protocol named as AVRP. (i.e.) Analyzed Virtual Routing Protocol. That resolves all the drawbacks in the MANET and Topological Networks. It Construct by using Artificial Intelligent Concept for protecting the system and network. It is suitable even for non-technical audiences.

2. RELATED WORKS

2.1. MANET:

A mobile ad hoc network is an infrastructure less multi-hop system of wireless autonomous mobile nodes. Reactive routing protocols like Ad hoc On Demand Distance Vector Routing (AODV) and Dynamic Source Routing (DSR) are appropriate for mobile environments, because they cope quickly with topological changes. Lately cooperative transmission- based routing protocols have been proposed to further save energy and enhance reliability.

However, they require an existing conventional route and individual addressing of the cooperating nodes, which involves a lot of overhead. In this paper, we propose a new Opportunistic Large Array (OLA) -based extension to AODV, which incorporates cooperative diversity into both route discovery and data transmission without requiring any pre-existing route or any individual addressing of relay nodes.

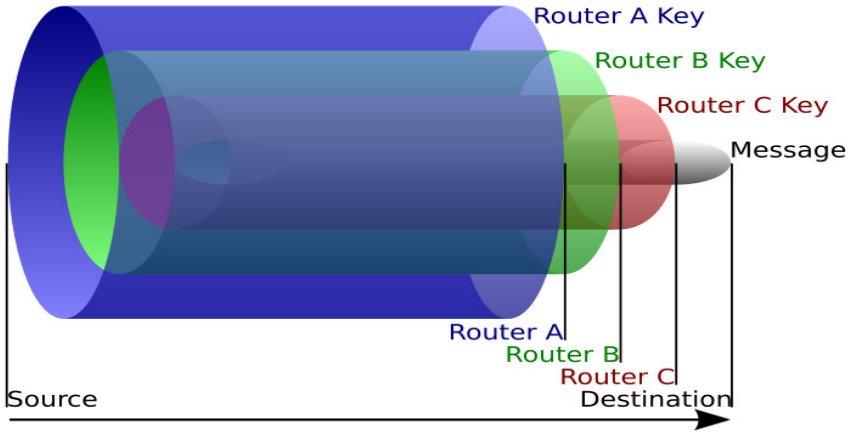
2.2. Back Pressure Restoration:

PBMRP–BR (position-based Multicast Routing Protocol for Ad-hoc Network Using Backpressure Restoration). For making the transmission and multimedia applications efficiently in Ad-hoc Network. This provides priority based path distance for routing, Load at the node (i.e., traffic) and queue length at the node (i.e., bandwidth). It also keeps the path information including bandwidth resources of each node for routing decisions. This backpressure restoration can be used to make the data transaction efficiently.

2.3. Onion Routing Protocol:

Onion routing is a protocol used to communicate for secured transaction of data in the network. It can transact the data using three layer key protections. In this protocol, the message is hidden and transmitted. It is a routing protocol technique anonymous communication over a computer network. The idea of onion routing is to protect the privacy between the sender and receiver on the computer network.

It is an end-to-end communication service. Messages are repeatedly encrypted and then sent several network nodes. Onion accomplishes that the data travel from the sender to the receiver by the sequence of proxies that reroutes the data to an unpredicted path.



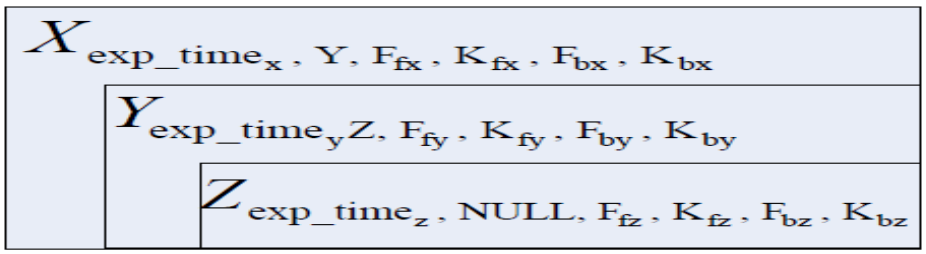
Architecture of Onion Routing Protocol

Weakness:

- Timing Analysis.
- Intersection Attack.
- Predecessor Attack.
- Exit Node Sniffing.

2.4. Onion:

The onion data structure is composed of layer upon layer of encryption wrapped around a payload. Leaving aside the shape of the payload at the very center, the basic structure of the onion is based on the route to the responder that is chosen by the initiator's proxy. Based on this route, the initiator's proxy encrypts first for the responder's proxy, then for the preceding node on the route, and so on back to the first routing node to whom he will send the onion.



A Forward Onion

When the onion is received, each node knows who sent him the onion and to whom he should pass the onion. But, he knows nothing about the other nodes, nor about how many there are in the chain or his place in it(unless he is last). What a node Px receives looks like this.{exp_time, next hop, Ff, Kf, Fb, Kb, payload} PKx Here PKx is a public encryption key for routing node Px, who is assumed to have the corresponding decryption key. The decrypted message contains an expiration time for the onion, the next routing node to which the payload is to be sent, the payload, and two function/key pairs specifying the cryptographic operations and keys to be applied to data that will be sent along the virtual circuit. The forward pair (Ff, Kf) is applied to data moving in the forward direction. (Along the route the onion is travelling) The backward

pair (Fb, Kb) is applied to data moving in an opposite direction (along the onions reverse route). (If the receiving node is the responder's proxy, then the next hop field is null). For any intermediate routing node the payload will be another onion. The expiration time is used to detect replace, which pairs of compromise nodes could used to try to correlate messages. Each node holds a copy of the onion until exp_time. If he receives another copy of the same onion within that time he simply ignores it. And, if he receives an onion that has expired, he ignores that as well.

2.4. MALBACO :

Multi-Agent Load Balanced Ant Colony Optimization Algorithm. Mobile ad hoc networks do not have any fixed topology. Routing in such network is very challenging and difficult due to the mobility of the nodes. Ant colony optimization is an efficient optimization technique used to find the optimum shortest route on the ad-hoc network.

2.5 ZRP for MANET:

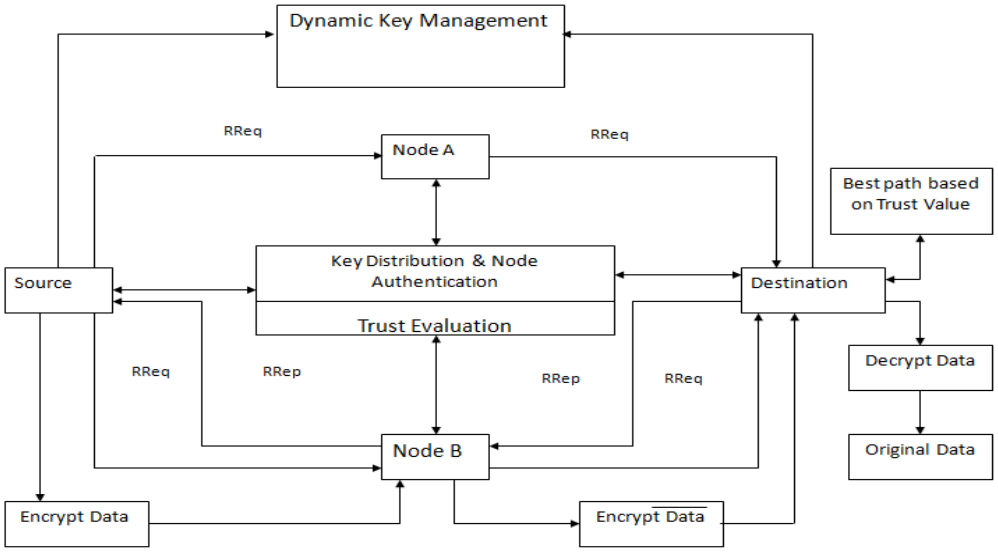
ZRP is Zone Routing Protocol (ZRP). It is a framework. Proactively maintains routing information for a local neighborhood (routing zone), while reactively acquiring routes to destinations beyond the routing zone. This is the First hybrid routing protocol which can be more efficient than traditional Zone Routing Protocol (ZRP) framework for both the proactive and reactive routing component. The ZRP cannot provide the expected reduction in the control traffic. These techniques can be applied to single or multiple channel mobile ad-hoc networks to improve both the delay and control traffic performance of ZRP. This ZRP Protocol can reduce the control overhead of PRP (Proactive Routing) and decrease the latency caused by the route discovery in RRP (Reactive Routing Protocol).

2.6. Tracing the Malicious Nodes in MANET :

Here in this paper, we have done an investigation and mathematical analysis based upon the detection of malicious nodes with attack modeling .We propose a scanning procedure and security measures for the multi-hop wireless network after diagnosis the abnormal behavior of malicious node and verify the physical presence of attacks strategy in a wireless network.

2.7. Byzantine Attack:

Byzantine attacks can be defined as attacks against routing protocols, in which two or more routers collude to drop, fabricate, modify, or misroute packets in an attempt to disrupt the routing services. First, how to detect and defend internal attacks against routing protocols, such as Byzantine attacks, has been a particularly challenging problem.



Structure for Byzantine Attack:

The problem has often been avoided by most secure routing protocols by assuming that the nodes should be trusted once authenticated. However, a MANET cannot use such a CA server. Third, the existing practice in developing secure routing protocols is by first establishing a PKI and then using cryptographic primitives to protect the messages exchanged in the routing protocols. The security and routing mechanisms are separately designed to meet the conflicting requirements: security requires using intensive computations, whereas routing needs to be efficient to properly scale. Thus, the resulting protocols may be secure but not feasible or vice versa.

2.8. Watchdog Intrusion Detection Systems:

Watchdogs are the basis of different Intrusion Detection Systems. They have the advantage of using only local information and therefore, they are robust to most of the attacks. Although importance of this mechanism is clear, it is hard to and studies that seriously test the watchdog in wireless mobile scenarios with high degrees of mobility, a characteristic of any Mobile Ad Hoc Network (MANET). In this work we demonstrate that an extra effort must be done to solve some watchdog drawbacks that are still present when using them in MANET scenarios.

2.9. OLSR MANET PROTOCOL:

Optimized Link State Routing (OLSR) protocol is a proactive Mobile Ad hoc Network (MANET) routing protocol. Security aspects have not been designed into the OLSR protocol and therefore make it vulnerable to various kinds of attacks. Recent research efforts have focused on providing authentication and encryption techniques to secure the OLSR protocol against attacks from outside intruders. Protocol semantics checking Any abnormal protocol semantics will trigger an intrusion alarm. While we use OLSR as an example, we argue that the presented approach can be applied to any Multi-Point Relay (MPR) proactive MANET protocol

2.10. Jamming Mitigation in Wireless Multihop Networks

Wireless networks are susceptible to localized disruptions, due to the shared nature of the medium. Radio jamming, the most common type of localized disruption causes wireless link failures. Jamming mitigation has been traditionally addressed in the physical and MAC layers. Such approaches come with added complexity and often require specialized hardware. We investigate whether a generally applicable routing layer approach, based on multipath routing coupled with power control, can mitigate the effects of jamming. We propose (1) proactive protection and (2) reactive protection techniques for jamming mitigation in wireless multi-hop networks with fixed nodes. For reactive protection, we propose a distributed geographic routing algorithm that finds alternative route to the destination, starting from the first node with failed link on the original path.

2.11. MOBILE AD-HOC NETWORK CAPACITY AND POWER EFFICIENCY

Specifically the problem addressed is to determine how the capacity of a MANET can be increased by the optimal placement of an additional dynamic node in a power efficient manner. This node is envisaged to be a platform whose primary purpose is to increase the capacity and power efficiency of the MANET.

Given a specific network configuration the optimal location of an additional node is investigated. This node insertion is teamed with power adjustments of all the nodes carried out in a manner consistent with topology control technique described can significantly decrease the jamming experienced within a MANET, thereby increasing the network's capacity. Additional benefit is also observed in the power usage of the MANET falling, thereby increasing the operational lifetime of the network. From the results obtained it will be inferred that a simple distributed algorithm to find the optimal point is not a trivial exercise.

3. Construction:

3.1. AVR PROTOCOL:

This routing protocol is nothing but the combination of some specified protocol. Signal, Bandwidth, Speed, Security, Redundancy, Durability & Recovery, Hacking are the some of the problems that are not recoverable in the internet. This Analyzed virtual routing protocol overcomes those problems. Here, the data encrypted by the user's system. After, the modem performs the duplication; the hackers trace the modem means it produce the duplicate data only. After transmission by the AVR protocol, it multiplies the duplicated data into lakhs of duplication. The lakh of duplicated data are transmitted on the virtual layers. In this, the original data has mixed with the dummy data.

The Following Steps are

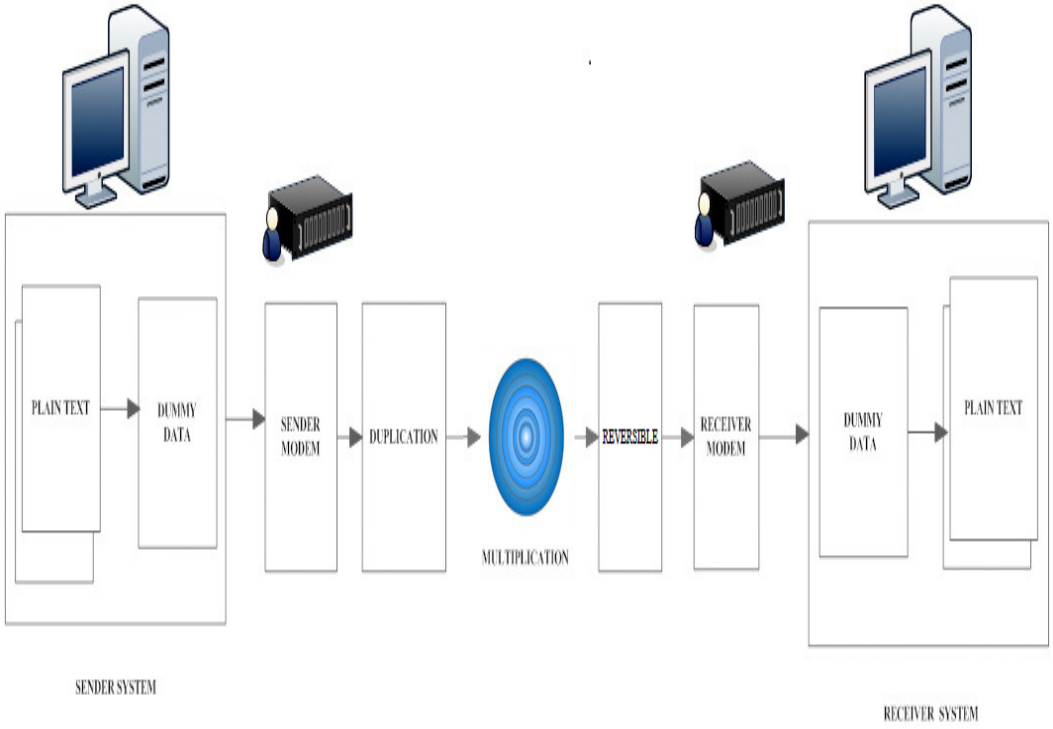
1. Encryption.
2. Duplication.
3. Multiplication.
4. Reversible and
5. Decryption.

Important problem:

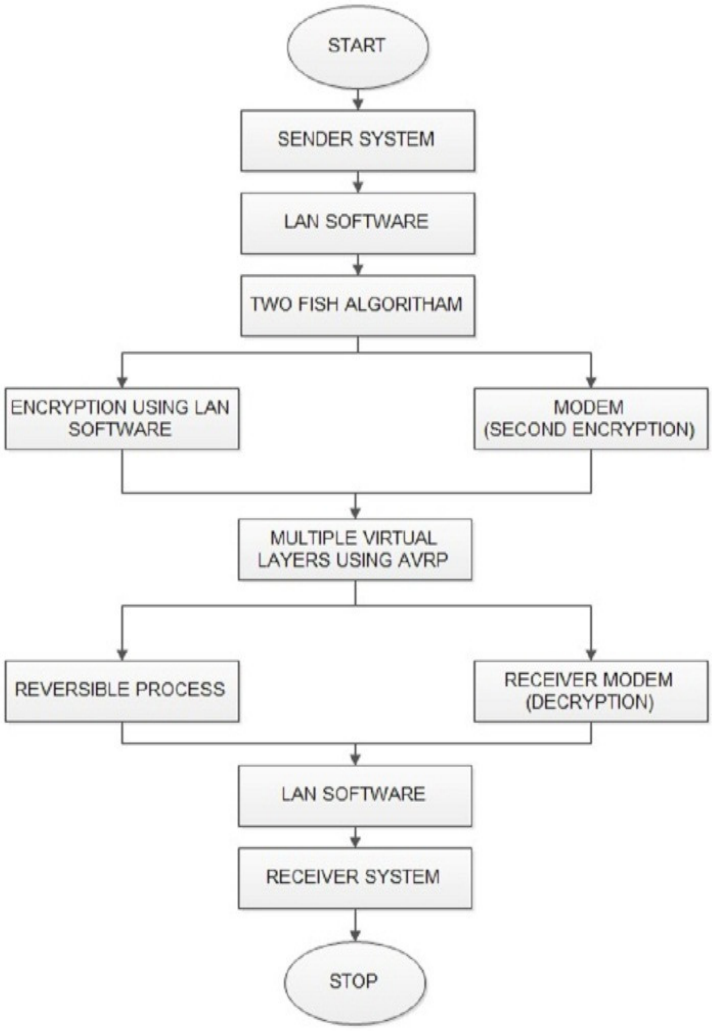
Internal attack (i.e.) Byzantine Attack- It Attacks against Routing Protocol. If the hackers trace the protocol, it also wastes of time.

3.2. AVR Protocol Schema:

This schema is going to explaining the overall process about AVR Protocol. Because protocol is a set of rules can perform the task by the given condition. As well as in AVR Protocol that consists of some rules that precede a safe transaction in the network.



Architecture of AVRP



Flow diagram for AVRP

3.1. Encryption

Encryption is the conversion of data into a form, called a cipher text, which cannot be easily understood by unauthorized person.

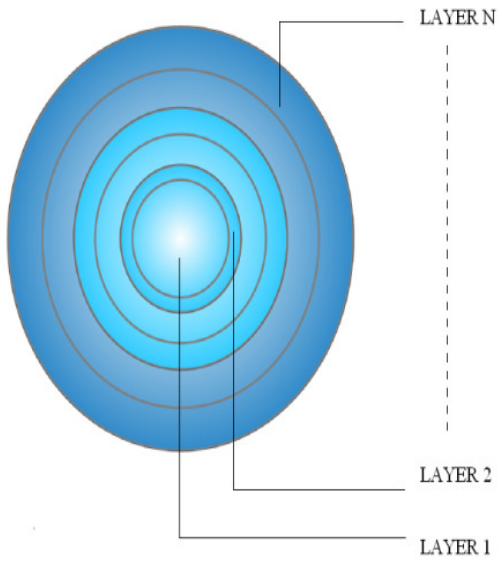
The Special thing in this encryption there is no protection keys. Because the hackers are, try to unlock the key to view the protected data, so no protection key rendered on encryption. In this encryption process, the data's are first encrypted on system one time. It saves the data into your drive for backup and it protects in the system itself after it moves to the modem. Here it has against encrypted the same data. That method named as Duplication.

3.2. Duplication:

Duplication is the process of dummy data for the original data. It performs on modem. (i.e.) the self-encrypted data performs encryption again on modem. It is used to protect the original data in common way. Now the data will be encrypted in double time.

3.3. Multiplication

Multiplication is a process where it performed by the middleware operation that the encrypted data traveled on the AVRP protocol. Here the duplicated data can make a lakhs of layers in a form of virtual topological network method.



Multiplication operation in AVRP

It creates a dummy layer on AVRP protocol. Here the duplicated data will be multiplied into lakhs of duplicated data. Here the hackers can try to capture the data by the method of flashing techniques, now the captured data will viewed by lakhs of data. However, the protocol can transfer 500k per second. Now the data capacity is may be 2500 (or) 7500 k per second. Therefore, the hackers cannot able to find the data. Here the data will be secured on AVRP protocol. This is a highly secured method in this paper.

3.4 Reversible

Reversible is preprocessing of decryption, which is an end part of this AVRP protocol. In this reversible part, the duplicate data decrypted here by the method of reversible order. On the receiver side, the data automatically convert into reversible by based on the time (i.e.). It changes the reversible by dynamically. By receiving on modem, it makes the same duplication process. After receiving from the system, it decrypts the data by the receiving system.

Here the special operation is that the reversible can reverse the data by different ways i.e. Front (or) rear (or) middle. Mainly this operation used to confuse the hackers to get a duplicate data for failure action. Reversible code decrypts the data at the end of the receiver system only.

3.5 Decryption

Decryption is the process of converting encrypted data back into its original form, so it understood. Encryption / decryption are especially important in wireless communications. This is because wireless circuits are easier to tap than their hard-wired counter parts. Never the less, encryption / decryption is a good idea when carrying out any kind of sensitive transaction, such as a credit-card purchase online, or the discussion of a company secret between different departments in the organization.

The stronger the cipher that is the harder it is for unauthorized people to break it the better in general. However, the strength of encryption /decryption increases. In this project, we use the encryption in the receiver's system with acknowledge. By using this type of encryption techniques, the hackers cannot be able to hack the information during the data transformation.

4. Result and Analysis

4.1 Comparison between AODV and AVRP:

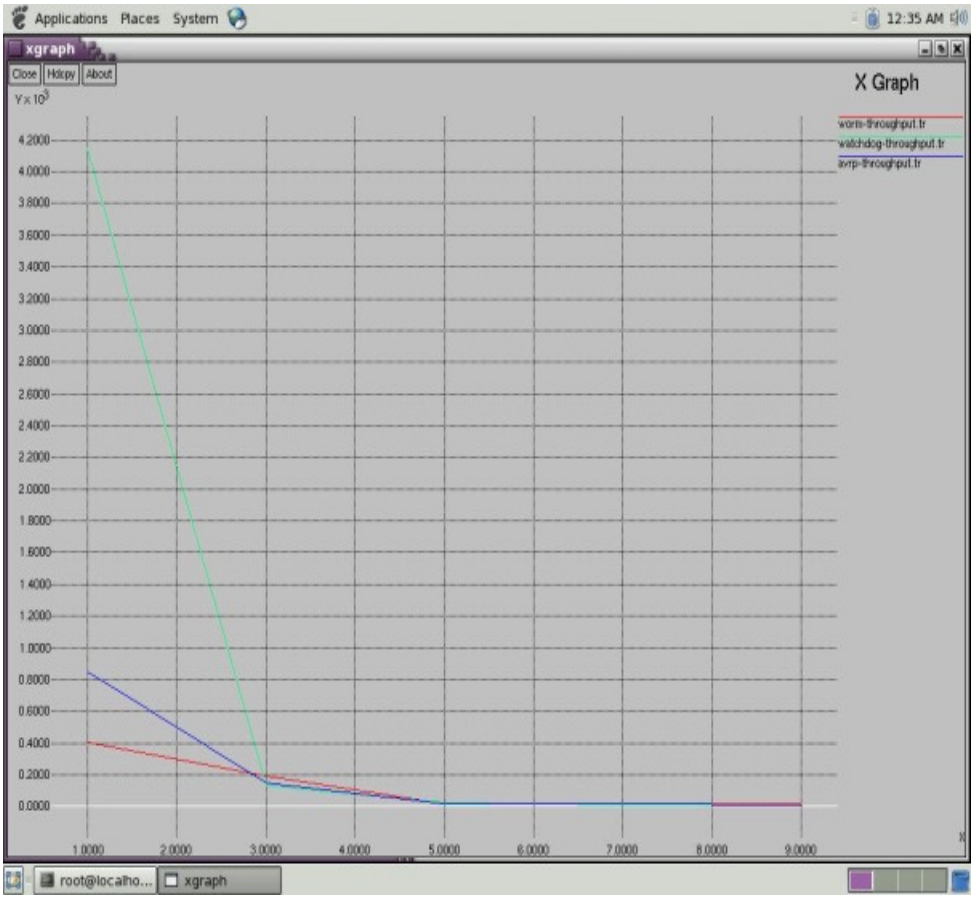
At present, the most reliable protocol compared to others is AODV. AODV (Ad-hoc on demand distance vector routing protocol) is a reactive mobile Ad-hoc network routing protocol. The AODV protocol is more comfortable compared to other protocols. This packet routing protocol specially designed for MANET. The AODV protocol is a UDP based protocol. This can able to handle more than 100 of the nodes.

In this, the source address and the destination address are defined previously by using their IP address. If the destination address not available, this precedes a route discovery mechanism to find the destination address. A routing table is maintained in the protocol, which has contained the details about the destinations that has reached in the data transmission route. However, the routing table contains limited memory to maintain the information details about the destination node.

Therefore, this cannot able to maintain the entire details about the data-transferring path. It contains two phases discovering the route and maintaining the route. Before route discovery origination, the destination node has increments the sequence number of that data transformation. The data delivery has more comfortable with using this AODV protocol. RREQ, RREP, RERR, and HELLO are the message types of AODV. The route request message contains the route table for the intermediate nodes of the network for communication. Route reply uses the route table to for reach the destination easily

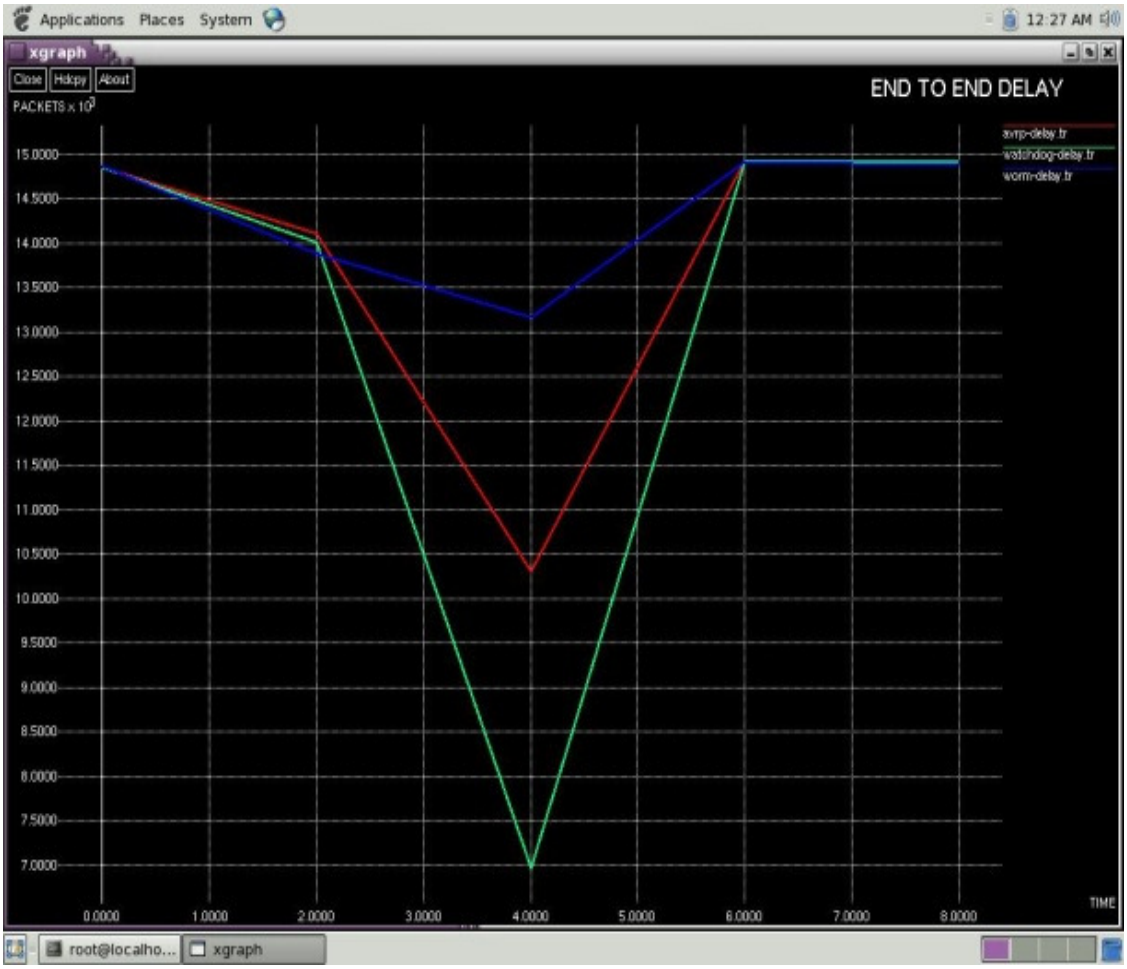
Here, the intruder attack makes a packet transaction error. The source has received an error message (RERR). At that time, the packet transaction range becomes zero. This makes the interruption between sources to destination. Here, we use an AVRP protocol to solve those problems, because the AVR protocol is transferring the data in a duplicated way. The duplicated data have travelled via the multiple layered protocols. The original data and lot of duplicate data are travelling on the protocol. The percentage to identify the original data is zero. If, the packets are not reaching the destination at the correct time, the packet transformation from source to destination has been delayed.

In the AVRP network, we use an internal node to identify the intruders and the attackers. That name as WATCH DOG node. This identifies the packet droppers and hackers. This provides the maximum range of security compared to the AODV protocol.



Throughput of AODV and AVRP

The variation of both protocols is shown in the graph. The graph shows the signal range in the normal, and using AODV and AVRP. Comparing the throughputs of AODV and AVRP in intruder attack. In this throughput graph WATCHDOG THROUGHPUT.tr is the successive output of the throughput graph is an better when compare to other throughputs of worm and AVRP.



End to end delay of AODV and AVRP

When, the packet is transferred continuously without any interruption, the delay of the network from source to destination is not occurred on the connection. The end-to-end delay of the AVRP less compared to the AODV. The end-to-end delay proof is projected in the graph.

CONCLUSION

If this concept is implemented means then our network will be highly secured network. If this concept is implemented in our real world means, our network is being an unleashed.

ACKNOWLEDGEMENT

Our sincere thanks to professor's Mr. Kannaiya raja, Mr. Radha Krishnan and developing engineers Mr. Deepak and Mr. Arun from Matrix cube technologies for make the project perfectly.

REFERENCES

[1] *Toby Xu, Ying cai.*2007. Streaming in MANET: Proactive Link Protection and Receiver-Oriented Adaptation.

[2] Umang Patel, Trisha Biswas, Rudra Dutta. . A Routing Approach to Jamming Mitigation in Wireless Multihop Networks.

[3] Shobha.K.R, Dr.K. Rajanikanth.2009. Efficient Flooding Using Relay Routing in On-Demand Routing Protocol for Mobile Adhoc Networks.

[4] A.K. Daniel, R. Singh, Zubair Khan. 2010. Position Based Multicast Routing Protocol for AD-hoc Wireless Network Using Backpressure Restoration.

[5] Ditipriya Sinha, Rituparna Chaki.2009. MALBACO - A New Multi-Agent Load Balanced Ant colony Optimization for MANET.

Authors

[1]R.Viswanathan received the certification of Diploma in Computer Science Engineering from Pallavan polytechnic college on 2009. Now following B.E computer science Engineering Arulmigu Meenakshi Amman College of Engineering Kanchipuram and affiliated on Anna University.

[2]J. Vignesh Kumar received the certification of diploma in Computer Science Engineering from Pallavan polytechnic college on 2009. Now following B.Tech information technology in Maamallan institute of technology sriperumpudur and affiliated on Anna University Chennai.

[3]T.V. Krishna Prasad received the certification of diploma in Computer Science Engineering from Bakthavatchalam polytechnic college on 2008. Now following B.Tech information technology in Maamallan institute of technology sriperumpudur and affiliated on Anna University Chennai.