International Journal Of
Recent Scientific
Research
ISSN: 0976-3031
Volume: 7(4) April -2016

SECURE ROUTING USING ALERT PROTOCOL IN MANETS WITH KEY EXCHANGE MECHANISM

Subashini B., Anto Bennet M., Abinaya T., Banupriya J.A and
Jelcin Renis J

THE OFFICIAL PUBLICATION OF
INTERNATIONAL JOURNAL OF RECENT SCIENTIFIC RESEARCH (IJRSR)
http://www.recentscientific.com/ recentscientific@gmail.com

ISSN: 0976-3031

Available Online at http://www.recentscientific.com

International Journal of Recent Scientific Research
Vol. 7, Issue, 4, pp. 10004-10010, April, 2016

International Journal of Recent Scientific Research

Research Article

SECURE ROUTING USING ALERT PROTOCOL IN MANETS WITH KEY EXCHANGE MECHANISM

Subashini B[1]., Anto Bennet M[2]., Abinaya T[3]., Banupriya J.A[4] and Jelcin Renis J[5]

[1,2,3,4,5]Department of ECE , VELTECH, Chennai, India Chennai-600062

ARTICLE INFO

Article History:

Received 05th January, 2015
Received in revised form 08th February, 2016
Accepted 10th March, 2016
Published online 28st April, 2016

Keywords:

Notify and go, hierarchical partitioning, destination zone, replication attack, polynomial bivariate key

ABSTRACT

Mobile ad hoc networks (MANETS) are very useful in establishing communication among a group of soldiers for tactical operations. Setting up of a fixed infrastructure for communication among a group of soldiers in enemy territories or inhospitable terrains may not be possible. As the military applications require very secure communication at any cost, the vehicle mounted nodes can be assumed to be very sophisticated and powerful. Anonymous routing protocols that hide node identities and routes from outside observers in order to provide anonymity protection are used. The existing anonymous routing protocols rely on either hop-by-hop encryption or redundant traffic, which either generate high cost or cannot provide full anonymity protection to data sources, destinations and routes. ALERT protocol offers high anonymity protection to sources, destinations and routes. However, it does not serve as bulletproof to adversaries. So, in addition we use a key exchange mechanism, that verifies the identities of the random forwarders that act as temporary source for the transmission dynamically, hence the transmission becomes more reliable and effective. The protocol achieves anonymity of source, destination and route at lower cost. We theoretically analyse the protocol in terms of anonymity, average delay and packet delivery ratio.

INTRODUCTION

With the growing needs of Mobile telecommunication devices with dynamic topology, MANETS (Mobile Ad hoc Networks) have become a popular area of research and have been emerging with advanced technologies. Being an infrastructure less network system, MANETS actively participate in the communications in which the connection establishment and connection termination occur on the fly. Therefore, MANETs are quite suitable for military applications and other law enforcement operations. Many protocols are being designed for MANETs. Since they are employed in military applications, communication security and provision for source and destination anonymity have become the essential features that the protocol should possess. As MANETs comprise mobile nodes and common radio channel, resource constraints are needed to be considered while designing a protocol for MANETs. With the advancement in technologies that provide security, the methods which counteract those security provisions i.e., network security attacks also occur widely in MANET environment. Providing anonymity for source and destination is not the only necessary action to make a network robust enough against such attacks. The route through which the data packets have been passed through should also have anonymity i.e., dynamic routing should be employed.

Among the anonymity providing protocols ALARM (Anonymous Location Aided Routing in suspicious MANETS) uses the location of source and destination for transmission instead of their identities thereby providing identity anonymity to source and destination. ZAP (Zone-based Anonymous Positioning routing protocol) focuses only on providing destination anonymity. ALERT (Anonymous Location-based Efficient Routing protocol) comprises features which are capable of providing identity and location anonymity to source and destination and route anonymity.

Anonymity Providing Strategy

In our proposed work, we use ALERT protocol for providing source, destination and route anonymity. ALERT protocol does not come under the protocols which rely on hop-by-hop and redundant traffic mechanism. As these mechanisms are not used, resource constraints problems are less worse when compared to other security providing protocols. Therefore, ALERT provides very secured communication in MANETs at low cost. Thus combating all types of attacks.

*Corresponding author: **Subashini B**
Department of ECE, VELTECH, Chennai, India Chennai-600062

Source anonymity

Source anonymity is provided in ALERT protocol using “Notify and Go mechanism”. This is nothing but the node (source node) which has data packets to be sent to another node (destination node) notifies its neighbours that it is going to transmit shortly. On getting this notification, the neighbours after waiting for a particular time interval (the time during which the source starts to send data packets), start sending dummy packets in order to provide source anonymity.

Route anonymity

Route anonymity is provided by hierarchical zone partitioning and by generation of dynamic routes for each transmission even if the source and the destination nodes are the same. According to the density of the nodes (ρ) , the size of network area (G) and the number of nodes in the destination zone (k) ,the number of partitions to be made (H) is determined using the formula below,

$$H = log_2\left(\frac{\rho \cdot G}{k}\right)$$

The protocol first partitions the network into H partitions. The partition is done in horizontal and vertical manner alternately. The first partition is made such that the source and destination nodes are not in the same zone. After the partitioning task gets completed, in each zone a Random Forwarder (RF) is chosen through which the data packets would be sent during the transmission. Incase, if the RF in a zone is out of range of the RF of the previous zone, transmission to the new RF is achieved through relay nodes. ALERT protocol uses GPSR algorithm for transmission between RFs.

Destination anonymity

As in ZAP protocol the destination anonymity is provided by the creation of a destination zone. Using the geographical location of the destination node, a destination zone is created. The RF chosen at the destination zone broadcasts the packets to be sent to the destination zone, to all nodes that reside in the destination zone at that time thereby providing destination anonymity.

Alert’s resilience to security attacks

ALERT protocol has resilience to timing attacks and intersection attacks.

Timing attacks

For a passive attacker, who observes the transmissions that are going through the network, it is possible to guess the source and destination nodes by closely focusing the time interval between the transmission start time at the source and the reception time at the destination for various transmissions. It occurs when the same route is generated for the same pair of source and destination. In ALERT, timing attack is prevented by the dynamic routing strategy.

Intersection attack

In ALERT, the destination anonymity is provided through formation of destination zone. Even though the broadcast of packets destined for the destination zone, provide destination anonymity, there are possibilities that the passive attacker be able to guess the destination. The observer compares the existence of nodes in Z_D (Destination zone is referred as Z_D) for a number of transmissions, finds the intersection of those node sets, thereby finding the destination node. therefore to counter this attack

ALERT provides destination anonymity through two steps. First the packets are multicasted to a set of nodes by the RF. Care should be taken that that node set does not include the destination zone. The nodes which receive the packets hold those packets until they receive the next set of packets. As soon as they receive the next set of packets, they perform one-hop broadcast of the previously received packets do that they reach the destination by the second step.

Proposed System

Unlike wired systems, which has dedicated routers for packet forwarding, MANETs do not have such dedicated nodes, a node can act as a host as well as a forwarder. ALERT selects the random forwarder in each zone without any authentication. Therefore, there exists a chance that the random forwarder may not be a reliable node. An adversary node can perform replication attack. We propose a system, as an enhancement to ALERT with a key exchange mechanism to overcome this replication attack. We use AODV (Ad hoc On-demand Distance Vector routing) algorithm, for the transmission of packets instead of using GPSR (Geographic Perimeter Stateless Routing) algorithm.

Replication attack

The mobile node is captured physically by some adversary. Once it is captured, adversary collects all the credentials like key and identity etc. The attacker can reprogram it and replicate the node in order to replace eavesdrop the transmitted messages or compromise the functionality of the network.

We classify sensor network attacks into three main categories.I dentity Attacks, Routing Attacks & Network Intrusion. Identity attacks intend to steal the identities of legitimate nodes operating in the sensor network. The identity attacks are Sybil
4 attack and Clone (Replication) attack. In a Sybil attack, the WSN is subverted by a malicious node which forges a large number of fake identities in order to disrupt the network’s protocols. A node replication attack is an attempt by the adversary to add one or more nodes to the network that use the same ID as another node in the network.

Steps to remove replication attacks

1. First, replica nodes should be detected with minimal communication and computational overheads.
2. Second, the detection schemes should be strong and highly resistant against an attacker’s attempt to break them.
3. Finally, only compromised and replica nodes would be detected and revoked. This implies that the attacker should be prevented from turning a replica detection scheme into a tool for denial of service attacks.

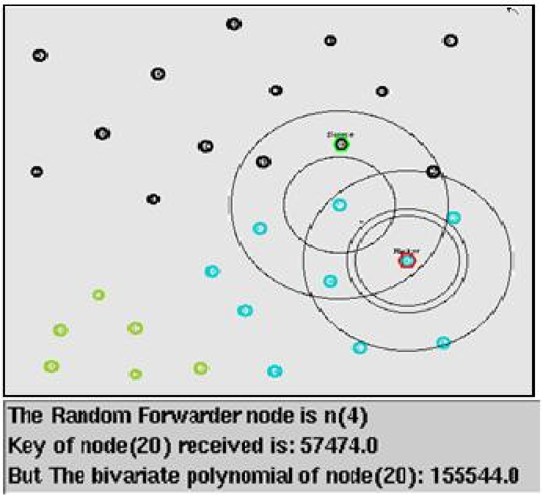
Polynomial Bivariate Key Generation

The bivariate polynomial is generated by using the following equation. The polynomials have the property of P(a,b)=P(b,a).

P (a, b) = $\sum_{0}^{t}{}_{<i,j<t} c\,(ij) a^i b^j$, c (ij) =c (ji)

Where, c (ij) denotes communication cost
a ,b denote the node ID

A polynomial pool is dynamically generated. Each node in the system is assigned a polynomial which has been generated using the above mentioned formula.



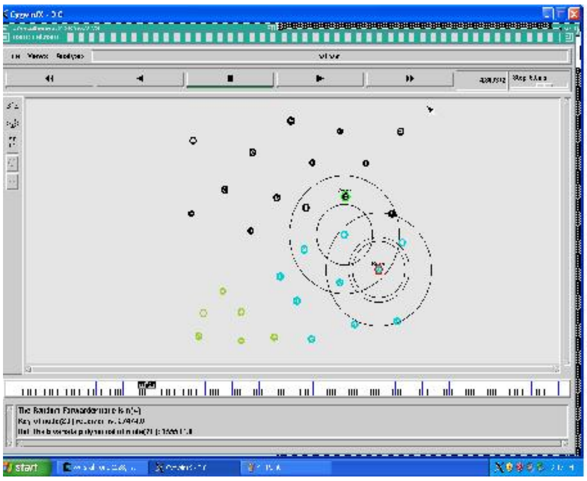
The Random Forwarder node is n(4)
Key of node(20) received is: 57474.0
But The bivariate polynomial of node(20): 155544.0

Fig.1 Key verification using bivariate polynomial key

Using this property it provides authentication for the nodes. When a random forwarder needs to chosen the node which has data packet to forward exchanges its pseudo ID with that of the node chosen as an RF . Both the nodes generate the key . If the keys generated by both the nodes are the same, the node forwards packet to the chosen RF or thinks it as an adversary node and eliminates it from the routing path. Another node is chosen as RF and the key exchange checking procedure is repeated. This prevents the intrusion of an adversary node in the transmission.

Simulation and Analysis Of Alert Using Ns2

We have analysed the results of our proposed system using NS2 software and produced related graphs on the analysis.



The Random Forwarder node is n(4)
Key of node(20) received is: 57474.0
But The bivariate polynomial of node(20): 155544.0

Fig.2 Screen shot showing key verification

Network Simulator (NS) is a simulation tool targeted at both wired and wireless (local and satellite) networking research. NS is a very promising tool and is being used by universities and researchers. In this report we provided information how to install NS2 on UNIX and Windows. A simple but limited method is to combine the existing components with OTcl scripts; a complex but powerful method is to implement new components into NS2 using C++. NS2 uses the combination of C++ and OTCL for programming. It uses C++ for backend and OTCL for frontend programming. It also includes provision for graph generation, animation visualization and event scheduling.

SIMULATION RESULTS

Simulation results are analysed using four parameters, which is of major concern to the protocol's efficiency and implementation. They are namely,

- Packet loss ratio
- Packet delivery ratio
- Packet delay
- Average Packet Delay.

Parameter description

Packet loss ratio: It gives the number of packets lost at a given time. Packet loss occurs when one or more packets of data travelling across a computer network fail to reach their destination. Packet loss is distinguished as one of the three main error types encountered in digital communications; the other two being bit error and spurious packets caused due to noise. Packet loss can be caused by a number of factors including signal degradation over the network medium due to multi-path fading, packet drop because of channel congestion,[1][2] corrupted packets rejected in-transit, faulty networking hardware, faulty network drivers, or normal routing routines (such as DSR in ad hoc networks [3]). Packet loss can also happen intentionally through network dissuasion technique for operational management purposes. When caused by network problems, lost or dropped packets can result in highly noticeable performance issues or jitter with streaming technologies, voice over IP, online gaming and videoconferencing, and will affect all other network applications to a degree.[5] However, it is important to note that packet loss does not always indicate a problem. If the latency and the packet loss at the destination hop are acceptable then the hops prior to that one don't matter.

Packet delivery ratio: The ratio of the number of delivered data packet to the destination. This illustrates the level of delivered data to the destination.

∑ Number of packet received / ∑ Number of packet sent

The greater value of packet delivery ratio means the better performance of the protocol. PDR is the acronym for Packet Delivery Ratio. It is the measure of all the packets successfully arrived to receiver (destination).
Packet Delivery Ratio,
PDR = {(Total number of data packets successfully reached the receiver) / (Total number of data packets transmitted)}* 100

Packet delay: Packet Delay is the measure of time taken the packet to move from its source to destination.

Average Packet Delay: Average Packet Delay depends on factors like the collision of packets and also the congestion because of number of connections in a given network .The Packet Delivery Ratio and Average Packet Delay are inversely proportional to each other. Because Packet Delivery Ratio is high, the number of packets received are more and hence the delay is small to receive higher number of packets in the network.

Analysis of simulation is done using graphs generated for,

- Thirty nodes scenario
- Forty nodes scenario
- Comparison of both scenarios comprising thirty and forty nodes

Thirty nodes scenario

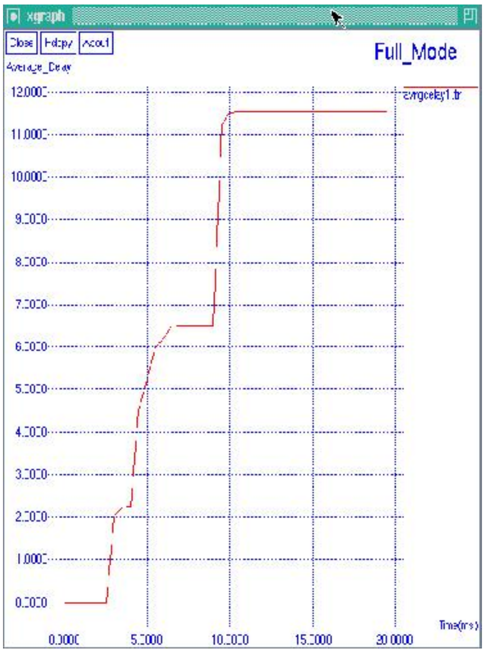


Fig.3.1 a. Average delay

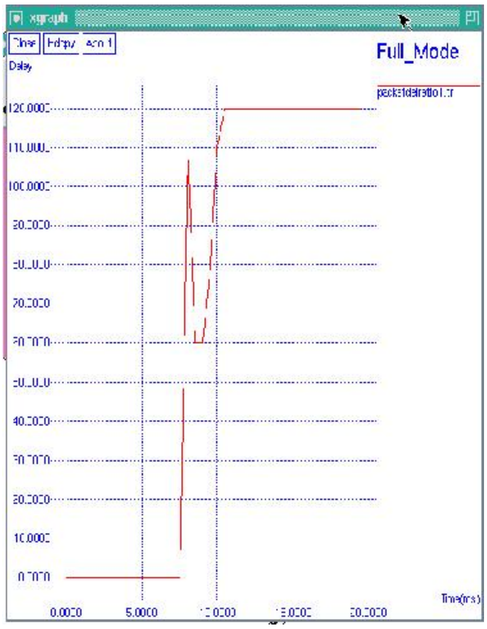


Fig.3.1 b. Delay

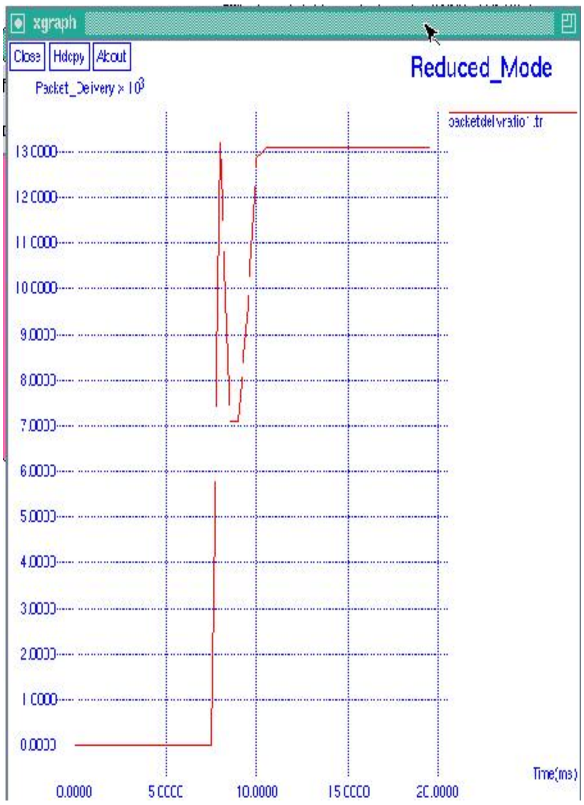


Fig.3.1 c Packet delivery

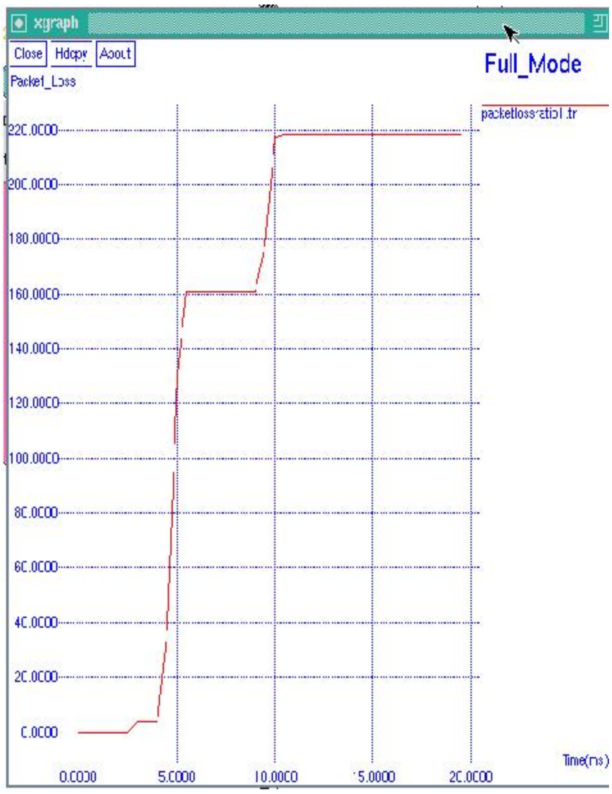


Fig 3.1 d Packet loss

Fig. 3.1 Graph analysis for thirty nodes scenario

7 Forty nodes scenario

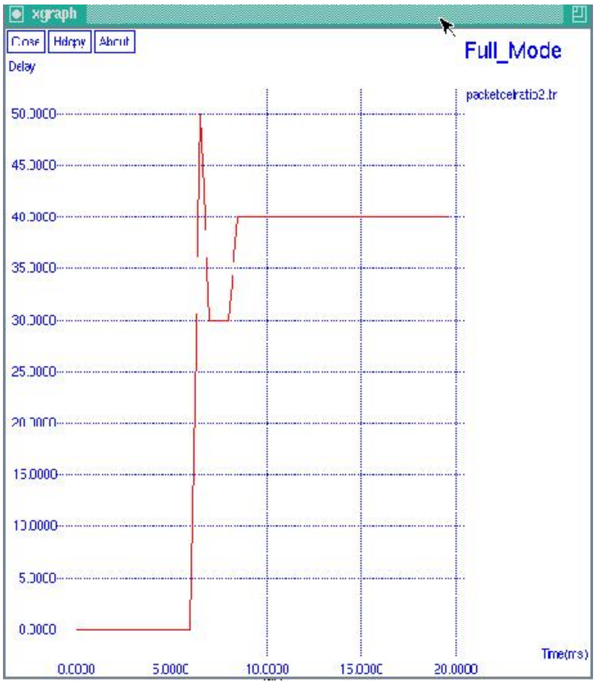


Fig 3.2 a Packet delay

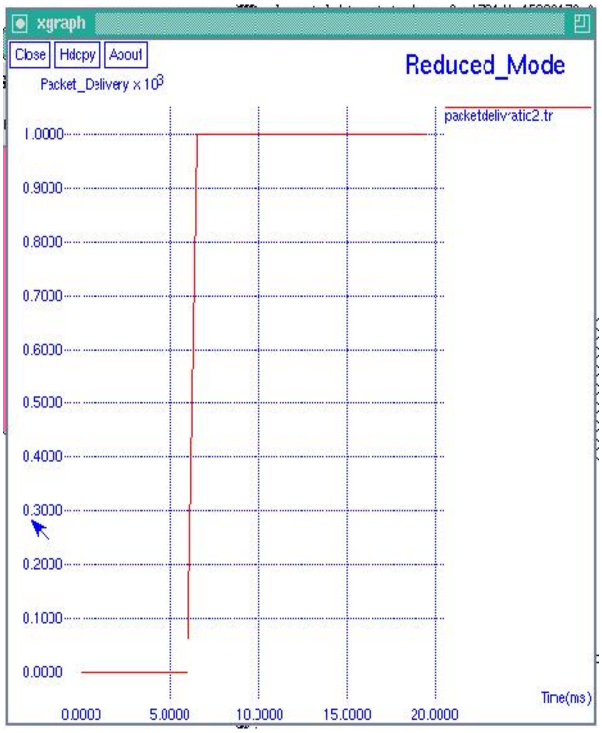


Fig 3.2 b Packet delivery

Future Work

We would like to use one-way hash chain algorithm for authentication an analyse the simulation results. One-way chains are an important cryptographic primitive in many security applications. As one-way chains are very efficient to verify, they recently became increasingly popular for designing security protocols for resource-constrained mobile devices and sensor networks, as their low-powered processors can compute a one-way function within milliseconds, but would require tens of seconds or up to minutes to generate or verify a traditional digital signature. Recent sensor network security protocols thus extensively use one-way chains to design protocols that scale down to resource-constrained sensors. A one-way function is a function that is easy to compute on every input, but hard to invert given the image of a random input. Here "easy" and "hard" are to be understood in the sense of computational complexity theory, specifically the theory of polynomial time problems.

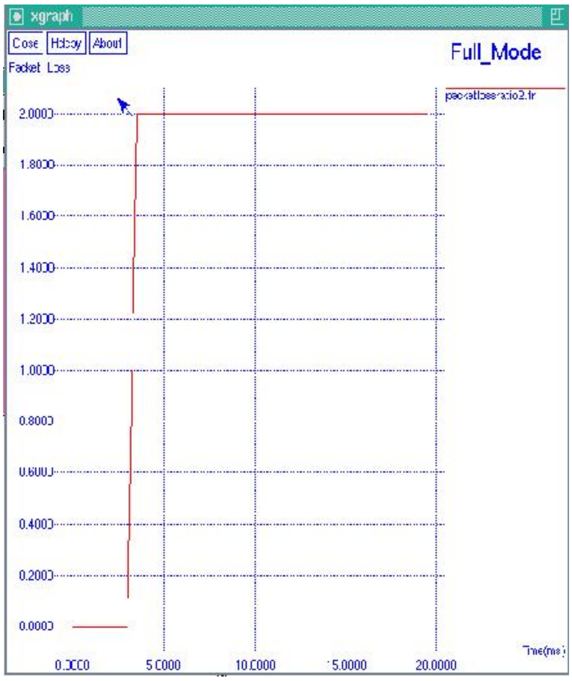


Fig 3.2 c Packet loss

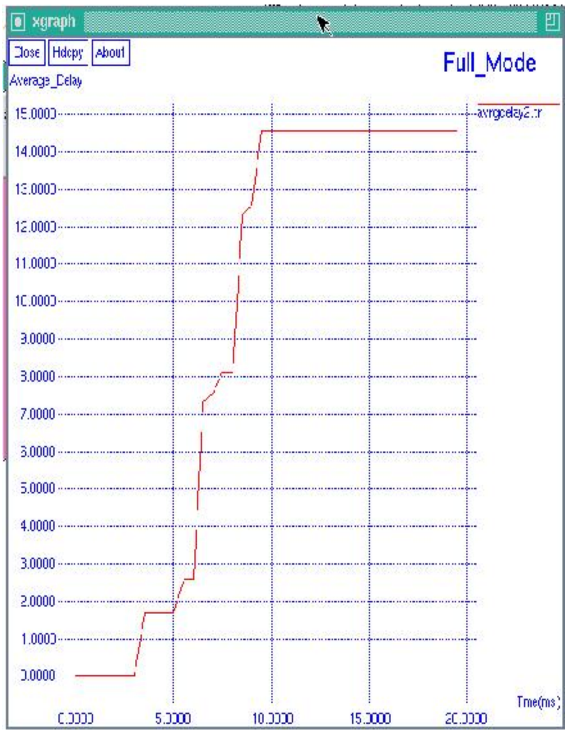


Fig.3.2 d Average delay

Fig. 3.2 Graph analysis of forty nodes scenario

Comparison of two scenarios

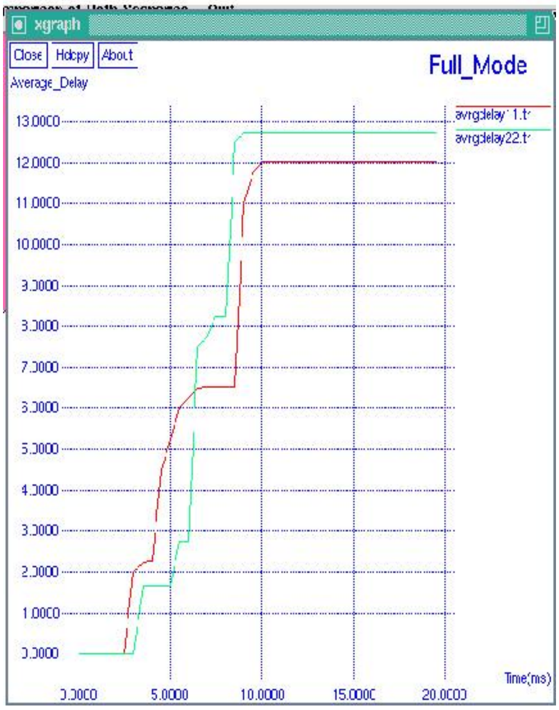


Fig 3.3 a Average delay

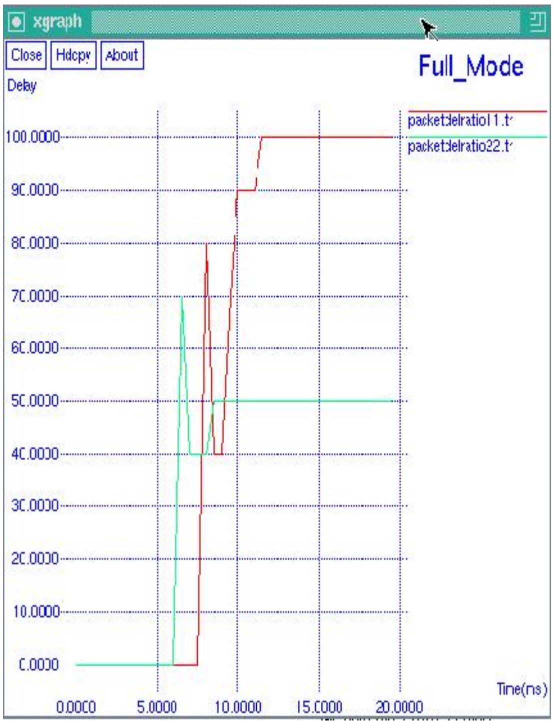


Fig 3.3 b Packet delay

Not being one-to-one is not considered sufficient of a function for it to be called one-way hash chain is the successive application of a cryptography hic hash function to a piece of data. In computer security, a hash chain is a method to produce many one-time keys from a single key or password. For non-repudiation a hash function can be applied successively to additional pieces of data in order to record the chronology of data's existence.

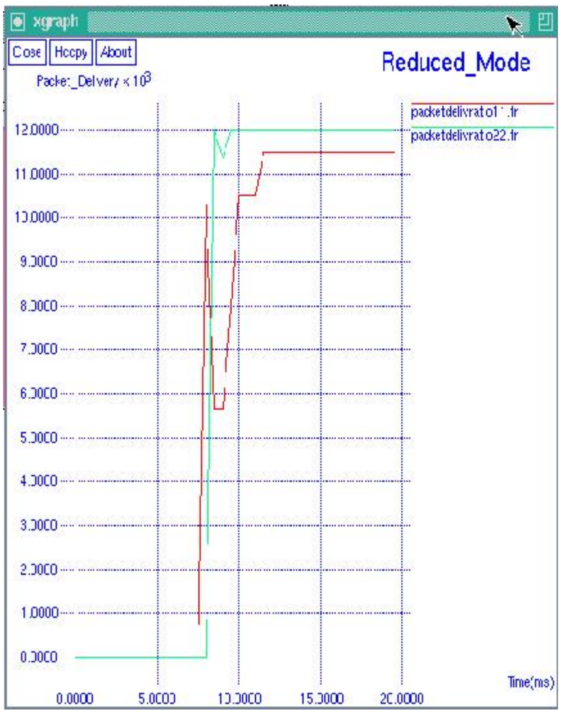


Fig 3.3 c Packet delivery

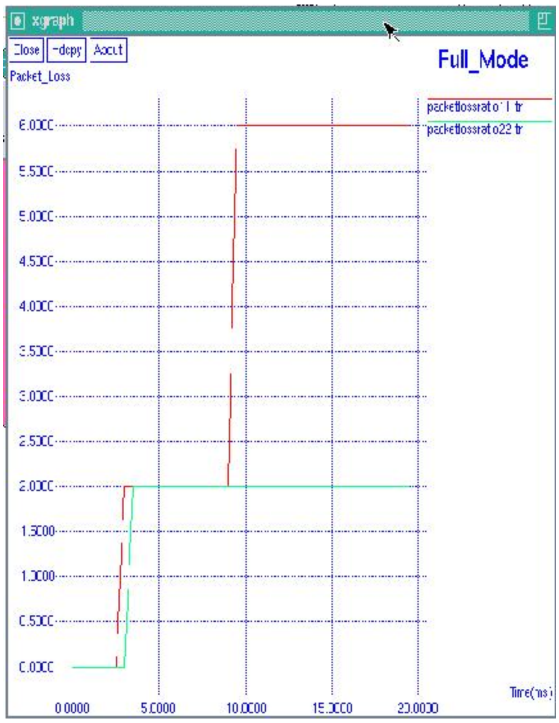


Fig 3.3 d Packet loss

Fig 7.3 Comparison of graphs of thirty and forty nodes scenarios

A hash chain is a successive application of a cryptographic hash function to a string. For example,

$h\left(h\left(h(h(x))\right)\right)$ gives a hash chain of length 4, often denoted.

CONCLUSION

Previous Anonymity providing protocols rely on either hop-by-hop encryption or redundant traffic and generate high cost .The existing anonymity protocols provide anonymity to either the source, the destination or the route .In contrary to the existing protocols, “Secure routing in MANET’s using ALERT protocol with key exchange mechanism” provides anonymity to all three essential insecurity prone criteria of the network .In addition to this ,the protocol combats the adversaries trying to obtain the data or information being transmitted ,by dynamically generating keys based on polynomials .The key exchange takes place in the same manner as that of the data. Thus it ensures a secure mode of data transmission without being affected by any adversaries. The protocol on the other hand is completely reliable and effective, providing a secure routing with minimal cost. The experimental analysis clearly demonstrates that the shortcomings of other similar existing anonymity providing protocol can be overcome by this protocol. The routing efficiency is high compared to other routing protocols. Thus the protocol can efficiently meet the requirements of military application, where data security is of prime importance .Further more work is required in implementing the simulation in real time. With advancement in technology, this work can be enhanced and has a wide scope in military communications.

References

1. Pfitzmann, M. Hansen, T. Dresden, and U. Kiel, Anonymity, Unlinkability, Unobservability, Pseudonymity, and Identity Management a Consolidated Proposal for Terminology, Version 0.31,”technical report, 2005.
2. Eitan Altman and Tania Jimenez, “NS Simulators for begginers, lecture notes 2003-2004”, Univ. de Los Andes, Merida, Venezuela and ESSI, Sophia-Antipolis, France.
3. Ruma Kareem Ajeena, Hailiza Kamaruihaili and Sattar B. Almaliky, “Bivariate polynomials public key encryption schemes”, *International journal of cryptology research* 4 (1): 73-83 (2013)
4. Sk.Md.M. Rahman, M. Mambo, A. Inomata, and E. Okamoto, “An Anonymous On-Demand Position-Based Routing in Mobile Ad Hoc Networks,” Proc. Int’l Symp. Applications on Internet (SAINT), 2006.
5. V.Manjula and Dr.C.Chellappan,” Replication attack mitigations for static and mobile WSN”, *International Journal of Network Security & Its Applications* (IJNSA), Vol.3, No.2, March 2011

****

How to cite this article:

Subashini B *et al.*2016, Secure Routing using Alert Protocol in Manets With Key Exchange Mechanism. *Int J Recent Sci Res.* 7(4), pp. 10004-10010.

ISSN 0976-3031

9 770976 303009 >