www.ijecs.in
International Journal Of Engineering And Computer Science ISSN:2319-7242
Volume - 3 Issue - 8 August, 2014 Page No. 7601-7604

Review of ALERT based on cryptography method

Kanmani.P[1] Dr. Y.Kalpana[2]

[1] M.phil Research Scholar, School of computing sciences, Vel's University, Chennai – 600 117.
Email: kanmani_214@hotmail.com

[2] Associate Professor, School of computing sciences, Vel's University, Chennai – 600 117.
Email: ykalpanaravi@gmail.com

ABSTRACT

Mobile Ad Hoc Networks (MANETs) make use of advanced network routing protocols that categorize the notes and manage the communication of packets. ALERT (Anonymous Location - Based Efficient Routing Protocol) has remained highly efficient in terms of efficiency and maintenance of consistency. ALERT protocol is now applied to the packet communication to achieve secured encryption and decryption of data. This can also help in achieving a high degree of security within the network. ALERT based on cryptography proves to be reliable for multipath transmission in networks of varied complexities.

Index terms- Cryptography, routing protocols, ad hoc networks

1 INTRODUCTION

A number of wireless applications have evolved in the recent times due to the rapid developments in the area of Mobile Ad hoc Networks (MANET).MANET remains highly supportive and compatible to applications belonging to different fields. One particular issue with MANET lies in the anonymity of data sources and destinations. This issue has raised questions and added complexities to the process of communication in this network.

Anonymous Location-based and Efficient Routing protocol (ALERT) is a recently developed technique that attempts to manage anonymous routing and permits users to broadcast the data to target nodes without any hassles. While the anonymity is being protected, there still lies a problem in the node formation and encryption-decryption processes.

We have conducted experiments where the network communication is classified into two formats- direct, point-to-point links from sender to receiver and intermediate node communication. In order to intensify the security level, the storage capabilities are added to the destination nodes so that decryption takes place at the right time.

The remainder of this paper is as follows: In section 2, the existing ALERT protocol is reviewed. In section 3, the addition of cryptographic method to protocol is analyzed. In section 4, the conclusion and future works are presented.

2 ALERT Protocol

An ALERT can be of different network models with various node movement patterns such as random way model and group model. A MANET can be in a large field, which is used for node communication to reduce the communication latency.The location of a message's sender will be in transmission direction.When the sender communicates with other node; it shouldn't be traceable by any observer. Therefore, anonymous communication protocol can be used.

Untraceability communication: A malicious observer may try to block data packets, by sending a number of nodes or by tracing back to the sender [1]. However, the route should always be undetectable. A malicious observer also tries to detect destination nodes by placing an intersection attack.

2.1 ALERT algorithm

ALERT features with a dynamic and unpredictable routing path, which consists of dynamical and intermediate relay nodes. It has two partitions: horizontal and vertical. The upper part of the horizontal partition divided into two zones A1 and A2. The vertical partition zone traverses from A1 to B1 and B2. Then, the vertical partition zone B2 traverses to destination zone through random forwarded node. It can be shown in **FIG 1**. ALERT uses the horizontal zone partition and randomly chooses a node in partition zone as an intermediate relay node. It gives an unpredictable path for message type as shown in **FIG 1a.**

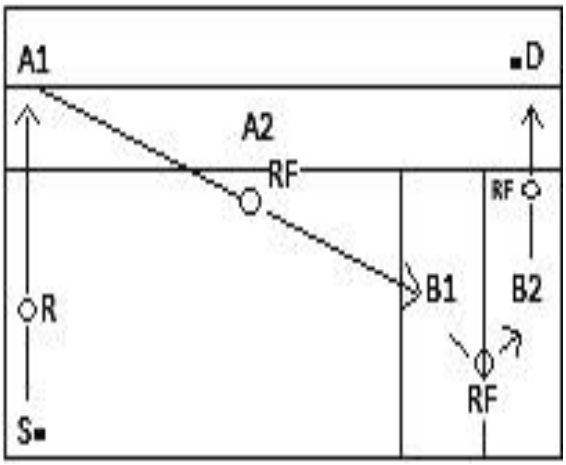

Fig 1. Routing among partition zone

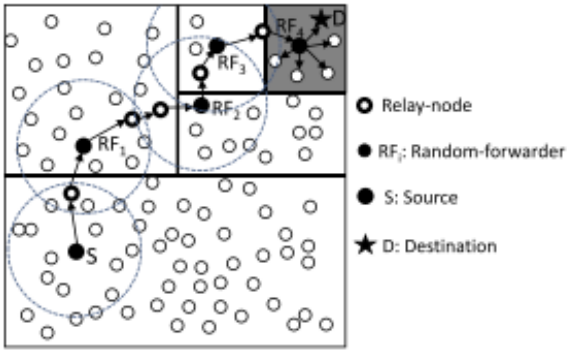

Fig 1a. Routing among zones in ALERT

2.2 Performance of ALERT protocol

-Number of actual participating nodes include RF's and relay nodes which participate in routing.

-Number of random remaining nodes provides high anonymity protection to the destination zone.

-Routing hop counts by number of packets sent, which shows efficiency routing algorithms.

-Average time in sending and receiving a packet reflects latency and efficiency routing algorithms.

-Fraction of second is taken to deliver a packet to destination.

3 Applying the Cryptography Method

The two techniques in cryptography are encryption and decryption. The option to manage the ALERT routing is for decryption technique processing and security. In this case, we have to use a private key. The receiver node has to decrypt packet thereby tightening the ALERT algorithm [2][3]. This procedure is shown in **FIG 2.**

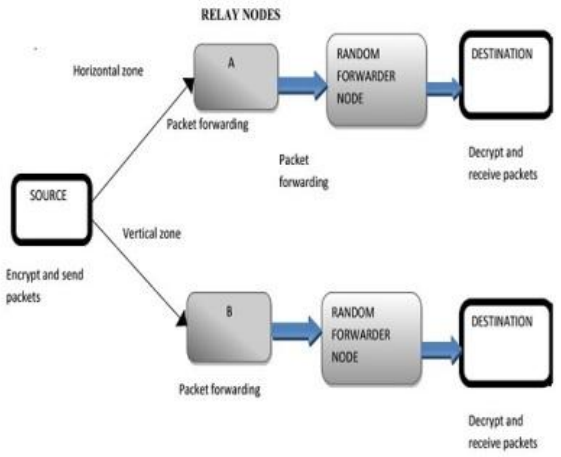

Fig 2: Applying the cryptography method

- From the source node, the horizontal and vertical zones packets are forwarded to relay nodes and then the packets are forwarded to random forwarder node and finally to destination node where it decrypts and receives the packets [3][4]. Source node contains the information of the packet. The packets are transferred from source part to relay nodes after encrypting the packets because the information should be transferred between source and destination. These encrypted packets are sent to random forwarder node. The information is eventually forwarded to the destination node by random forwarder node and the destination decrypts and stores the packets.

- Message forwarding is a forwarding technique in which information is sent to relay node where they forward to random forwarder node and send to final destination. In the ALERT routing, each data source/forwarder executes the hierarchical zone partition. It first checks whether itself and destination are in the same zone. If so, it divides the zone alternatively in the horizontal and vertical directions. The encrypted packets are received by the destination through relay node and random forwarder node from source.

- This ALERT routing technique has been done with the help of cryptographic algorithm (AES – Advanced Encryption Standard). The data has been given to the input file and it's initiated with AES algorithm for creating encrypt/decrypt mechanism on the same private key and forward to the nodes and reaches the destination. A secret value has been assigned to the input file. Once the data reaches to the destination zone, it remains on the encrypted format. It accepts the secret values from the receiver to decrypt the data and stores the data in to the specific location. [5].

4 CONCLUSION

ALERT protocol addresses the communication but doesn't handle the security. However, when we add the cryptographic mechanism, the packet doesn't get lost. It increases the efficiency and turn around time in a minimum rate. So, therefore cost is minimal.

ALERT routing technique strengthened the anonymity protection of source and destination by hiding the data with the help of cryptographic algorithm. Hence, it achieves the goal of being both secure and practical for real time systems.

ALERT Protocol in Cryptography can be further develop in cloud based vertical networks so that any number of users can use the system for various purposes in a secured way. Additionally, combination of cloud security mechanism with cryptographical technique will lead to accurate results. It reaches the

high level real time secure system for transferring data from source zone to destination zone.

REFERENCES

1. D. B. Johnson, D. A. Maltz , and Y.Hu , "The Dynamic Source Routing Protocol for Mobile Ad Hoc Networks (DSR)" 〈draft-ietf-manet-dsr-09.txt〉, April 2003

2. E. Royer and C-K. Ton, "A Review of Current Routing Protocols for Ad-Hoc Mobile Wireless Networks," IEEE Personal Communications Magazine, April 1999, pp. 46-55

3. B.Dahill, B. Levine, E. Royer, and C. Shields, "A Secure Routing Protocol for Ad Hoc Networks," University of Massachusetts Technical Report 01-37, 2001

4. B. Karp and H. T. Kung, “GPSR: greedy perimeter stateless routing for wireless networks,” in Mobile Computing and Networking, pp. 243–254, 2000.

5. P. Papadimitratos and Z. J. Haas, “Secure routing for mobile Ad Hoc networks,” in Proceedings of the SCS Communication Networks and Distributed Systems Modeling and Simulation Conference (CNDS 2002), pp. 27–31, 2002.