ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 5, Issue 6, June 2018

An Efficient Routing and Security Based on CBZA Algorithm

[1] S. Muneeswari, [2] N. Venkatesan
[1] PG Scholar, [2] Assistant Professor, Department of Computer Science and Engineering
Sri Vidya College of Engineering & Technology, Virudhunagar.

Abstract: MANET is one of the wireless Ad Hoc networks with wireless nodes under mobility. Due to its configuration and maintenance capabilities arises the security challenges in MANET. In this paper, an efficient routing with security based protocol towards mobile ad hoc networks is proposed. To provide security against malicious attacks an effective Cluster Based Zone Allocation (CBZA) algorithm is presented. Through NS2 simulations, the proposed CBZA method is compared with the MDR protocol. The proposed method achieves better reliability along with reduced energy consumption and improve the security also. Key generation is used for point to point and end to end communication achieved by Elliptic Curve Cryptography (ECC), is more scalable and requires lesser memory for storing keys. Also, the simulation results promises the detection of misbehaviour nodes and improved security.

Keywords: Mobile ad hoc network, Malicious attack, Attacker node, Group management, Zone allocation, Zone Leader, Elliptic Curve Cryptography (ECC), Vulnerability.

1. INTRODUCTION

A new technology improvement is made with a number of the necessities such as: reduction in size, low cost, consumes low power and distributed devices comparatively for brief and long distance communication. Wired networks are used for native process and wireless networks are employed for long distance communication. So as to produce such need, mobile unexpected networks for wireless communication that contains of a whole bunch or thousands of mobile nodes that are autonomous which has no physical infrastructure regardless of geographical locations;Therfore it provides service and access information altenative locations.MANETs are unit area adaptive and self organizing network. Where as the nodes utilized in MANETs should be able to notice the presence of alternative devices to alleviate the required discovered for communication. The adding and removing devices cannot have an effect on the network performance. It’s a ascendable network as a result of it accommodates the addition of additional nodes.

By the way, it provides additional flexibility. These are robust network since its no centralized infrastructure and that we will discovered the network at anyplace regardless of time. So as to support cluster communication, multicast is one in every of the foremost effective methodology when put next to unicast that may preserve the information measure and energy predominately.
.

In CBZA method, mobile nodes are formed as a cluster. By using cluster formation in MANET the security will be increased. First, we have to collect the relevant nodes to group the smilar nodes for cluster forming. Then give separate id to all nodes in the group management.second, allocate the Zone Leader for this cluster nodes. Depends up on the energy level and computation speed the Zone Leader is allocated. Third, in CBZA method misbehaving node should be easily identified during the packet transmission. In ECC cryptography, first identify all the misbehaving nodes and then recover the all misbehaving nodes through this cryptography.

2. LITERATURE SURVEY

In MANET, routing protocol is one of the security issues and different attacks on nodes, Reference [1] proposes a securing ad hoc protocols in a structured manner, we have classified them into two categories such as Solutions based on cryptography and one-way hash chain. By using cryptography the Secure Routing Protocol (SRP) developed by Haas is a protocol designed to secure the on-demand routing protocols that utilize broadcasting as its route querying method. By using one-way hash chain each node creates its hash chain by applying a one-way hash function to a random value. Hence, when a node sends or transmits a routing update, it includes one value from the hash chain for each entry in that update. Reference [2] proposes a performance analysis through different types of attacks, Packet Delivery Ratio:

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 5, Issue 6, June 2018

Percentage packets of message received by the destination node divided by sent by source node. Average End-To-End Delay: It includes all latency which is happened due to any reason like discovery of route, delay, queuing, re-transmission latency etc. at the transmission and other times. Throughput: It is defined as total packets received divided by duration of last packet received by destination node. It is calculated in bps "bits per second". Reference [3] proposes a role based approach secure routing, This approach enhances the flexibility and security of information flows in wireless ad-hoc networks. To implement SAR protocol, the QoP (Quality of Protection) bit vector should be used instead of the trust levels. Implementation of cryptographic protection is available on the basis of shared secret schemes. Reference [4] proposes a trusted based scheme against packet dropping attack, which is combination of social and QoS trust. The primary goal of our proposed scheme is to mitigate nodes performing various packet forwarding misbehaviors. We calculated four parameters for trust which are control forward ratio, data forward ratio, intimacy and residual energy. Reference [5] proposes a analysis of attacks in routing protocol, The routing in the MANETs is different from conventional infrastructure network since the nodes not only act as end devices but also act as routers. Owing to the resource constraint of the nodes the routing protocols for MANETs have to be light weight and assume a trusted environment. Reference [6] proposes a integrated key management, introduce an integrated KM-SR scheme that addresses KM-SR interdependency cycle problem. By using identity based cryptography (IBC), this scheme provides security features including confidentiality, integrity, authentication, freshness, and non-repudiation. Reference [7] proposes a identity-based multi-signcryption scheme, key distribution protocol not only can distributed threshold key in secure and efficient manner, but improves the availability of fully distributed threshold key management in MANET. Multi signcryption is an extension of signcryption for multi-users. Reference [8] proposes a threshold key management protocol, new ID based signcryption scheme which is efficient in terms of both the communication overhead and the computational requirement. Furthermore, apply our ID-based signcryption scheme into threshold key management. A system private key share refreshing protocol in threshold key management of a mobile ad hoc network is proposed. Reference [9] proposes a protocol architecture, for wireless networks that rely on significant Interactions between various layers (Cross Layer Design) of the network stack. A cross-layer approach to network design can significantly increase the design complexity. Indeed, protocol layers are extremely useful in allowing designers to optimize a single protocol layer design without the complexity. Reference [10] proposes a secure routing in integrated MANET, application of IBC to ad hoc networks for efficient key management and for the distribution of pair-wise shared keys among the authenticated nodes Providing secure Internet connectivity while the Mobile Node (MN) roams across different wireless domains operated by different agents and operators.

3. CLUSTER FORMATION AND ZONE LEADER ALLOCATION

In CBZA methodology a group of nodes are located into four regions and a Zone Leader is allocated to each region within the network. Relying upon the energy the Zone Leader is allocated. Suppose the energy is decrease the election method is continue and if two nodes have same energy then election method consistent with the processing speed.

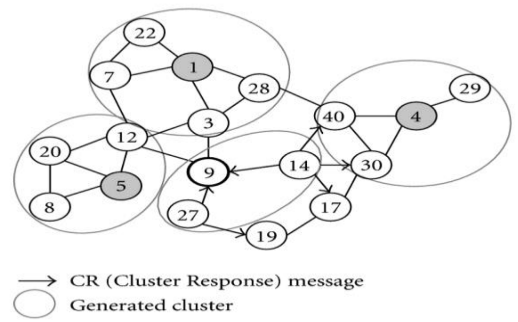

Fig 1: Cluster Formation

The Elliptic Curve Cryptography (ECC) is employed for key generation. Compared to symmetric key cryptography, ECC is more scalable, requires lesser memory for storing keys, introduces low communication overhead and is straightforward to deploy.

The packet transmission always takes place through the Zone Leader and this is the main process in cluster management. In this paper, proposed an algorithm for Cluster Based Zone Allocation method ology (CBZA) for energy conservation and reduce the packet dropping in Mobile Ad hoc Network. Finally, the performance of every region is evaluated.

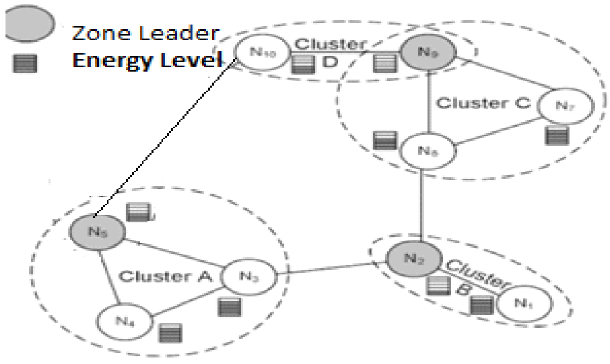

Fig 2: Zone Leader Allocation

3.1 Overview of CBZA

In Multipath Diversity Routing (MDR), once the path is failure it chooses the alternate link for packet transmission however in Cluster Based Zone Allocation technique (CBZA), zones are formed and packet transmission over routing method. In MDR, packet loss is increased owing to the link failure and packet delivery ratio is decreased. Then, end to end delay became very high. So, overall packet transmission time gets increased and overall network efficiency is reduced but in MDR, the detection of lost packet is somewhat crucial method. CBZA has low packet loss compared to MDR.

Normally in network infrastructure, nodes are deployed and source and destinations are allocated. Then, a one node can act as a router or agent. In cluster management, set of nodes are initialized at explicit region or four regions. Every region features a Zone Leader (ZL) and zone members. Zone Leader election is conducted among the nodes within the zone and a particular node will elected as a Zone Leader depending on its energy that is termed threshold value.

Except the Zone Leader alternative nodes can behave as neighbors or coordinators. Once the routing process/packet transmission is commenced through the network, each zone members are coordinated with one another and Request/Response method is performed by coordinators. Finally, each packet transmission like entering and exceeding packets is operated by the Zone Leader as a result of they are capable it. Then the on top of method is recurrent because the same.

3.2 CBZA Algorithm

Route Discovery β_{Sx}

Packets and ID's P_{id}

Set the threshold value (T_H= 45)

To Generate Secrete Key (Encode, Decode) Process

For Normal transmission

$\beta_{sx} \leftarrow T_H(x) + P_{id}$

For ($T_H = 0$; $T_H \leq N$; T_H ++)

If $T_H \leftarrow A$ // Satisfied the Threshold Value

Else $T_H \leftarrow B$ // Not satisfied the Threshold the value some threads injected

For Secure Transmission Process

Step:1 Secrete key generated

Encode key generated

$E_{id} \leftarrow \beta_{sx} + 1(x)$

$D_{id} \leftarrow \beta_{sx} + 1(y)$

Encode Security Key -1 $E_{id} \leftarrow 0x1hj@$ //Packet key injected Source Side

Decode Security Key -2 $D_{id} \leftarrow 0x1hj@$ //Packet key injected Destination Side Same Process following by coming Packet

Step: 2 Route Discovery

$\beta_{sx} \leftarrow E_{id}(x) + D_{id}(y)$

$\lambda S_{ix} \leftarrow \beta_{sx} + 1$ // Retransmission process

Step 3: Identify the Duplicate packet

$\beta_{sx} \leftarrow P_{id}(x)$

$\lambda S_{ix} \leftarrow \beta_{sx} + 1$

// Retransmission process the same

Step 4: Destination Side

$R_{ax} \leftarrow \beta_{sx} + \lambda S_{ix} + 1$

//Receive the Correct Packets reply the Ack.

4. EXPERIMENTAL RESULTS

In CBZA, when the zones are formed it splitted into four regions. The packet transmission takes place into the regions and when the transmission in first region is completed then only next region starts its transmission. Each region has a Zone Leader (ZL) which controls the packet transmission and reception through it. If the packet is lost, we can easily identify the lost packet in this method. So, the end to end delay and packet transmission time is reduced. By the way, we can increase the network throughput or efficiency.

TABLE 1. COMPARISON OF PARAMETERS

S.No	Parameter	MDR	CBZA
1	Total Number of Nodes	20	100
2	Total Number of Packets	1000	2500
3	Antenna type	Omni Directional	Omni Directional
4	Transmission Mode	Path Selection Process	Region Splitting
5	Bandwidth Ratio	0.9e6	2e6
6	Data Rate	0.96e6	2.0e6
7	Mobility	Dynamic	Dynamic
8	Density Rate	0.2	0.5

The Performance Metrics are compared as shown in Figures,

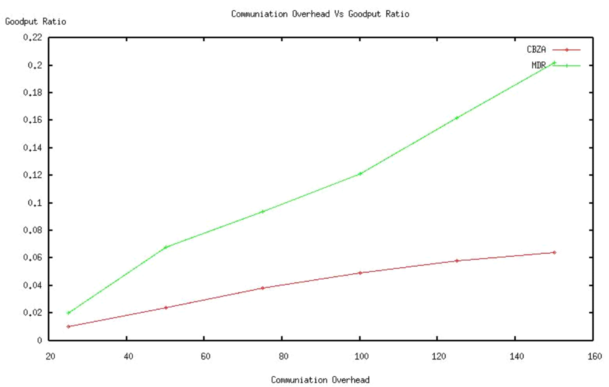

Fig 3: Comparison of Performance between communication Overhead Vs Throughput

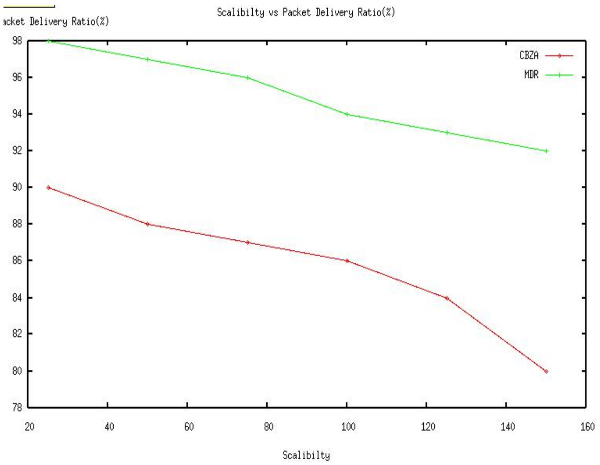

Fig 4: Comparison of Performance between Scalability Vs MDR

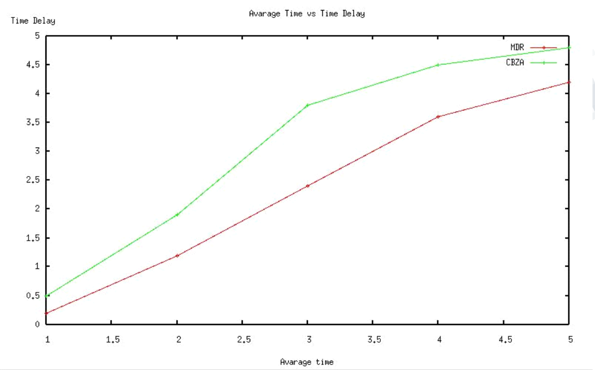

Fig 5: Comparison of Performance between Average Time Vs Delay

5. CONCLUSION

In this paper, a Cluster Based Zone Allocation (CBZA) algorithm is proposed to improve security, scalability. It is a group management process used in MANET. In CBZA method, packet transmission occurs into the zones so that the packet loss or packet drop is reduced and network error can be easily identified.

By splitting the zones, the energy consumption and network traffic are reduced; the network lifetime is increased to reasonable times. The packet transmission always takes place through the Zone Leader. When compared to MDR protocols this algorithm provides higher throughput and by the way overall network efficiency is increased and also increased the security for both routing and communication data. In future, on a simple mobile node platform to allow experimental observation and profiling of its performance, the proposal of network bridging solutions capable of providing services between two closed networks over an insecure intermediate network.

REFERENCES

[1] "Secure Routing Protocols for Mobile Ad HocNetworks",H.Moudni.,M.Errouidi.,H.Mouncif.,B.E.Hadadi, 2016.

[2] "Performance Analysis of Routing Protocols under Different Types of Attacks in MANETs", Lakshit Prashar., Raj Kamal Kapur, 2016.

[3] "A Role-Based Approach to Secure Routing in Wireless Ad-Hoc Networks", E.Shcherba.,V.I.Nikonov, 2016.

[4] "A Trust-Based Scheme against Packet Dropping Attacks in MANETs", Sachi N.Shah, Rutvij H. Jhaveri, 2016.

[5] " Analysis of Attacks on Routing Protocols in MANETs", Raj Kamal Kapur.,Sunil Kumar, 2015.

[6] "An Integrated Key Management and Secure Routing Framework for Mobile Ad-hoc Networks", Shushan Zhao.,Robert D. Kent., Akshai Aggarwa, 2012.

[7] "New ID-based and Threshold Key Distribution Protocol in MANET Using Multi Signcryption Scheme",Zhang Chuanrong, Zhang Yuqing, 2009.

[8] "Threshold Key Management Protocol in Mobile Ad Hoc Networks Using an ID-based Signcryption Scheme", Zhang Chuanrong., Xiao Hong, 2009.

[9] "Protocol Architecture for Mobile Ad Hoc Networks",P.Sai Kiran, 2009.

[10] "Secure Routing in Integrated Mobile Ad hoc Network (MANET)-Internet",K.Ramanarayana.,Lillykutty Jacob, 2007.

[11] "Multi-Path Security-Aware Routing Protocol Mechanism for Ad Hoc Network", In-Sungan, Hwang, Seok-Joong Cangl, 2006.

[12] "Identity-based Key Agreement Protocol for Mobile Ad-hoc Networks Using Bilinear Pairing", Hung-Yu Chien, Ru-Yu, 2006.

[13] "Performance Evaluation of Secuity- Aware Routing Protocols for Clustered Mobile Ad Hoc Networks", Gregory S.Yovan.,Kerem Erikci, 2004.

[14] "AODV Routing Protocol Implementation Design", Ian D. Chakeres, 2004.

[15] "Security Aware Adaptive Dynamic Source Routing Protocol", Shayan.,Okhta Ilghamin,Yaman,2002.