March - April 2020
ISSN: 0193-4120 Page No. 2027 - 2036

Secure Adaptive Request Zone based Routing Protocol for MANET

Vemuru Srikanth
Department of Computer Science and Engineering K.L. Deemed to be University
Green Fields, Vaddeswaram, Vijayawada Andhra Pradesh, India
G.T. Chavan
Department of Computer Science and Engineering K.L. Deemed to be University
Green Fields, Vaddeswaram, Vijayawada Andhra Pradesh, India
gt.chavan@gmail.com

Article Info
Volume 83
Page Number: 2027 - 2036
Publication Issue:
March - April 2020

Article History
Article Received*: 24 July 2019*
Revised*: 12 September 2019*
Accepted*: 15 February 2020*
Publication*: 18 March 2020*

Abstract

Mobile ad hoc networks (MANET) have some unique characteristics like infrastructure-less, hop by hop communication, and dynamic nature. Routing in MANET is very challenging because there are frequent route breaks due to node movements. To avoid the route request (RREQ) packet flooding storm during the route estimation phase, the Adaptive request Zone-Based Optimal Selective Forwarding with location (AZBOSF) routing protocol uses two zones namely request and expected. The RREQ packet is flooded in the request zone area, that determined by the source node during the route estimation phase. The expected zone is that area where the source node is expecting the availability of the destination node. This AZBOSF routing protocol adapts the request zone and expected zone dynamically with respect to length among the source and the destination node for achieving better performance. However, during the communication phase in the original protocol security mechanism is not considered. Being a wireless network, MANETs are susceptible to many attacks. The MANETs are generally application-specific, and if the application is like military, then security issue is very important. Hence for maintaining the secrecy and integrity of the data and to achieve the goal of trusted communication in this routing protocol, proposed a security mechanism using trust and identity with key management.

Keywords – *Zone-based routing protocols, MANET, Public key, Secret key, Request zone, Expected zone, Certificate..*

I. Introduction

The 'Location Aided Routing' (LAR) protocol decreases control overhead of path estimation by using position details of nodes in MANET. The protocol 'Zone-Based Effective Location Aided Routing (ZBELAR)' [1] uses the position information of both the nodes during routing. This protocol creates six zones of the overall network on the basis of angle. With respect to the angle of arrival, protocol decides the respective zone. The position details of the node are applied while the routing procedure. Whenever any source node initiates transmission to other nodes, it only considers the zone area of that destination node. This protocol considers each node is the 'Global Positioning System (GPS)' enabled for location information, but using GPS is not always advisable in MANET due to various reasons. It may not work properly in the indoor environment due to the line of sight and multipath fading problem, and cost increases with GPS antenna; position estimation error is still in a few meters, and energy of the mobile may be drain due to continuous reception of signals from GPS satellite. Hence the protocol Zone-Based Optimal Selective Forwarding (ZBOSF) uses a combination of

March - April 2020
ISSN: 0193-4120 Page No. 51 - 58

mobile nodes, that is with GPS and without GPS [2]. This protocol estimates the location of the non GPS nodes using the position details of the GPS nodes and the length between neighbors of the non GPS nodes in the initial phase. Hence ZBOSF protocol. reduces the number of GPS nodes in the network. Also, during the data transmission phase, this protocol works with LAR scheme 2. The protocol Zone-Based Optimal Selective Forwarding with Location (ZBOSFWL) [3] uses an improved DV-hop propagation technique for localization of the hosts in the MANET.

Parul tomar et al. [4] performed an adjective survey on safe routing protocols in mobile ad hoc networks, also authors discussed different attacks and proposed possible solutions to them. According to them, no one of the technique is capable of achieving whole security goals, hence recommended to a greater extent secure protocol that can consider the different necessities of mobile ad hoc networks. Ali Dorri et al. [5] surveyed security challenges in MANET. The authors defined three security parameters and discussed various defeating approaches against attacks. They analyzed different attacks like a black hole, warm hole, byzantine, snooping, routing, denial of service, jamming, man-in-middle, Gray hole, and traffic analyze. Also, given some proposed solutions like routing information, sniffing, redundancy, and dynamic frequency. According to them, routing information techniques are appropriate in every type of MANET. The sniffing technique is useful in the case of a single attack. K. Vijayakumar and K. Somasundaram in [6] performed a study on authentic and protected routing protocols in MANET. They considered various attacks as impersonation attacks, fabrication, attacks on modifications, and rushing attacks. The work provides the necessary ideas considering the capacity of attacks in MANET. Authors in [7] presented disputes and possible solutions to protected routing mechanism in mobile ad hoc networks.

The paper is organized into six sections. The second section describes the survey of existing literature. Section 3 describes the adaptive request zone-based routing protocol on which the security algorithm is applied followed by section 4 which gives a detail description of security procedure. Section 5 shows our simulation results and conclusion in section 6.

II. RELATED WORK

Vinay Kumar Pandey et al. [8] presented a Secure MANET Routing technique with Trust model (SMRT) routing protocol, which achieves privacy and security against inside and outside attackers. Basic operations of the SMRT routing protocol are similar to 'AODV (Ad hoc On-demand Distance Vector)' routing protocol, but it is a location-centric and secure one. Panagiotis Papadimitratos et al. proposed efficient, protected routing protocols in MANET [9-11]. Panagiotis Papadimitratos demonstrated the 'Secure Message Transmission (SMT)' protocol and it's optional, the 'Secure Single-Path (SSP)' protocol [12]. Yih-Chun Hu et al. have presented a new safe reactive routing protocol for MANET, referred to Ariadne [13]. It uses highly efficient symmetric cryptographic primitives for preventing compromised nodes or attackers of tampering on uncompromised paths and various Denial-of-Service attacks. Authors in [14] proposed an identity based protocol that secures AODV routing protocol and TCP communication in MANET. The projected protocol safeguards AODV by "Sequential Aggregate Signatures (SAS)" based on RSA. In this method, every node has a unique identity, that is measured from its shared key; nodes are not allowed to change their ID's throughout the network lifetime. Authors in [15] presented an innovative conception for planning an effective security answer that can defend the MANET of various attacks. The aimed "Secure Routing Protocol against Heterogeneous Attacks (SRPAHA)" protocol efficiently identifies and

March - April 2020
ISSN: 0193-4120 Page No. 51 - 58

secures the collaborative malevolent host without the demand for costly signatures.

P.Subbulakshmi and S.Vimal [16] proposed an 'Enhanced Identity-Based Cryptography (EIBC)' method to enhance the security in MANET. This method applies the cryptography concept for encryption and decryption of data packets alongside with routing information. EIBC system has secret values that execute similar to the original model secret value. In EIBC, the node estimates the live public key and live private key for verification purpose. Enhanced ID-Base signature is also applied for authentication rationale using the signature. After finishing the verification purpose, the protected channel transmits the data packets using Enhanced ID-Based Encryption. In Enhanced ID-Based Encryption, the node transmits the packet in an encrypted mode applying live public key, and the node receives the packet in a decrypted mode using a live private key. L. Raghavendar Raju et al. [17] presented a practiced and protected routing depended on asymmetric authentication practicing the 'Key Exchange Approach (KEA).' The projected method assures secure routing as well as QoS and reduces routing overhead in MANET.

J. Vijayalakshmi et al.discussed various methods of key management techniques for MANET [18]. A. S. Khubalkar and L. R. Ragha in [19] proposed security improvements to the 'Dynamic Source Routing (DSR)' protocol for allowing a reactive protected routing protocol, and they also suggested a procedure to interchange shared key amongst the source node and the destination node while the path establishment itself. A trustfulness based routing method for MANET is suggested by Vidhya P M and Ambily Mohan in [20]. This system estimates the global trust value of every node by applying direct and indirect techniques. According to the authors, the malevolent nodes could discover and eliminate from the network. The transmission among the nodes in the network must be carried out through the most trusted path. Jayanthi Chandrashekhar and Arun Manoharam in [21] presented a routing method, namely, 'Identity Based Key Management (IBKM)' for providing secure communication in MANET.

V. Lakshman Narayana and C. R. Bharathi in [22] proposed threshold cryptography that gives the authority more robust versus network calamities and more difficult to negotiate. Identity-based cryptography, where any identity can serve as a public key, makes certificates and certificate distribution supererogatory. They used the Private Key Generator (PKG) method for authority distributing private keys corresponding to identities. Jin-Hee Cho et al. proposed a completely disseminated confidence based shared key handling technique for MANET applying a soft security technique depended on the logic of trust, instead of applying tough hard security methods [23]. They proposed a 'Composite Trust-based Public Key Management (CTPKM)' intending to improve functioning during extenuating security threats. Every node applies a trust threshold to find the trust of another node. Poonam Saini and Shefali Aggarwal presented a trust value depended on the uncoordinated check pointing method in MANET [24]. They aimed to improve the total check pointing overhead obtained in the implementation of recovery techniques. They proposed a trust-value based check pointing method that considers the mobility of the node. The trust of the node depends upon its movement between the clusters.

III. ADAPTIVE REQUEST ZONE BASED ROUTING PROTOCOL

The 'Adaptive request zone Based Optimal Selective Forwarding with location (AZBOSF) routing protocol' [25]. In this protocol, for location estimation of the mobile nodes, the Ad hoc Positioning System (APS) algorithm [26] is used. This algorithm operates in three stages. In the first stage, the unnamed nodes (nodes which do not know their location coordinates) desires to get

March - April 2020
ISSN: 0193-4120 Page No. 51 - 58

their minimal hops to each reference node (landmarks) in the network by using the DV-hop propagation technique. Then in the second stage, the distance amongst node and anchor node is estimated. Finally, the unnamed node coordinators were calculated.

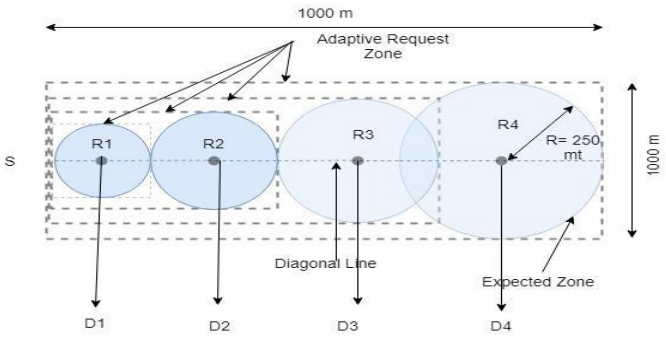

Fig. 1. AZBOSF routing protocol

Using the APS algorithm, when calculated node coordinates, authors in [27] claims that, that was not precise enough. Hence they proposed a sort of enhanced DV-hop method. This method works in two stages: 1. Average Hop-size Amend, and 2.Weight Matrix Calculation Coordinate. Hence for location estimation of the mobile nodes, this improved DV-Hop method is used in the AZBOSF routing protocol. This protocol is implemented to consider the adaptive request zone and motion of the nodes. Figure1describes the overall working of this protocol.

The distance amongst source mobile host S and destination mobile host is based on the diagonal line. For instance,

- If the gap is more than or equivalent to ¾ of the diagonal line, as of D4 in figure 4.13, then pick out the radius R4 as 250 meters. for estimating the expected zone area, this represents the distance among the destination host and source host is far away.
- When the gap is more than or equivalent to ½ as of D3, select the radius R3 as 187.5 meters for the expected zone.
- When the gap is more than or equivalent to ¼ as of destination node D2, then pick the radius R2 as 125 meters.

When both nodes are too near to each other like S and D1 node, then select radius R1as 62.5 meter.

Algorithms for Different Node:

The working of source node S is described in algorithm 1. While node S desires to transfer data, initially it finds out whether it has the position details of the destination node if it finds, it inserts this location details of the destination node and itself. Also, the timestamps are included

in the RREQ packet and broadcast it into the request zone

Algorithm 1. Working of Source Node

```
If Source node (S) wants to communicate with destination node (D1)
{       Lookup destination position in its PIT;
        If destination position in PIT is empty
        {       Broadcast route request message by using normal flooding mode
        Else if destination position in PIT is not empty
                Include its position and timestamp to route request message
                Broadcast route request message inside request zone
        else
                Include its position, destination node position, and timestamp in
                route request message.
                Broadcast route request message inside request zone
        }
}
```

Algorithm 2. Working of Intermediate Node: (During RREQ packet)

- When Xi gets RREQ packet, update a newer node position in PIT;
- Calculate source to destination distance and diagonal line and adapt radius;
- Calculate the request zone and expected zone and acquire node Ai location;

Check whether node Ai position is within request zone; if it in request zone, then forward RREQ packet to its neighbors towards destination direction; otherwise, drop the RREQ packet.

Algorithm 3. Working of Intermediate Nodes (During RREP packet)

- Node Xi gets RREP packet;
- Check node position in the packet;
- If the position is newer, then update its PIT.

March - April 2020
ISSN: 0193-4120 Page No. 51 - 58

Algorithm 4 depicts the working of the destination node. Whenever the node gets the route RREQ message, it sees its PIT for accessibility of the position information in it. If found, then it updates all entries like source nodes position and destination nodes position, also, it updates the timestamps of a message when it was sent and received. Every route request message contains the traveled route in its header information. Then it creates the route reply message and replies to the source node S on the chosen path with position and timestamps.

Algorithm 4: Working of Destination Node

```
If destination node D1 received the route request message;
    {if position information is available in message.
        {Update source and destination positions with
            timestamps in its PIT.
        Collect/Select a route by using route selection algorithm.
        Include position and timestamp itself in reply message.
        Send reply message back to the source via selected path.
        else,
            Collect/Select a route by using route selection algorithm.
            Send reply message back to the source via selected path.
    }
}
```

IV. SECURE AZBOSF (SAZBOSF) PROTOCOL

To attain the aim of trusted transmission in MANET various techniques by applying key organizations have been performed. Here a 'Composite IDentity and Trust-based model (CIDT)' rests on the physical individuality, trust of a host and public key that benefits in protected data transmission above wireless communication channels [28]. This CIDT model was applied to the DSR routing protocol, here we are applying on AZBOSF routing protocol to analyze the performances.

a. Trust Model

The Trust Factor (TF) of a host is rest on its effectiveness of data communication throughout its lifespan. The amount of packets thrown by the entire network or each node decides the transmission is successful or unsuccessful. The new node whenever entering into network, its trust is with another node is specified in the eq. (1).

$$TF_{m,n} = DTF_{m,n} + RTF_{m,n} \quad (1)$$

Where,

TF m,n : Trust of node *m* on node *n*.
DTFm,n: Direct Trust Factor of a node *m* on node *n* and it is calculated by *m* by directly monitoring the node *n*
RTFm,n: Indirect Trust Factor of node *m* on node *n* that is calculated later receiving the trust level of *n* from its 1 hop neighbor nodes.

The trust factor is being used for decision making, comprising gaining a certificate of distributing a public key, providing a public key requested and requesting a public key of a target node.

b. Composite IDentity and Trust based Model (CIDT)

CIDT is compound identity and trust-based model which rests on the identity of a node along with the

trust factor of a node in the network. A node in the network is identified by its key pair and its physical identity. The sub-processes that are executed in CIDT are as follows;

i) Key Generation

Each node in the network creates a key pair (PK, SK) for authentication and it is updated sporadically. The node in the network is described by its Public Key (PK), its identity (ID) and the Trust Factor of a node (TF) in the network. Composite Identity of the node is calculated by equation (2).

$$CID_{node} = f(PK_{node}, ID_{node}, TF_{node}) \quad (2)$$

ii) Certificate computation for a new node

When a new node N trying to join the network it sends its ID to the server node for the issue of a certificate to it for being a member of the network.

March - April 2020
ISSN: 0193-4120 Page No. 51 - 58

The server node authenticates the validity of the requesting node by testing for its *TFth (Trust Factor Threshold)* with the neighbors. Validity is a trusted certificate delivered to a node by its neighbor on successful verification. Validity factor between two nodes a and b is *validity (CIDb)* is the confidence of a that b is an authentic party. A node can be either a valid or invalid node. A certificate for the requesting node is produced for a definite time break after which it needs to be regenerated. The certificate *CERT* is computed as in equation(3);

$$CERT^{N}_{server} = SKserver\ (CIDserver, CID_N, validity, time) \quad (3)$$

Where,

$CERT^{N}_{server}$ - Certificate computed by server for node N
SKserver - Secret key of server node
CIDserver - Composite identity of server node
CID_N - Composite identity of new node N
Validity - Validity of Certificate
Time - Time period for which this certificate remains valid

iii) Public Key Propagation

When a host gets a certificate containing its public key, it sporadically propagates it to trusted one-hop neighbors. While propagating this packet, it must comprise. During this propagation the packet comprises of the following items:

$$(SK_N\ (CERT^{N}_{server}),\ PK_N)) \quad (4)$$

$CERT^{N}_{server}$ is a new host certificate. SK_N is a new host's Ns' secret key, and PK_N is a new host's public key.

iv) The Revocation and Update of key

The revocation of the shared or secret keys is carried out in two cases, one when time is expired and second if node founds a compromised node.

v) Node Authentication:

The following procedure shows the node authentication

n node in the network
M set of all nodes in the network
For all node n ϵ **M**
Check the validity of the $CERT^{N}_{server}$

If $CERT^{N}_{server}$ is valid
then authenticate node **n**
else
declare node **n** as unauthentic entity
Broadcast this message in the network

A valid node in the network is the authenticated node. After the authentication of the node, the message is broadcasted in the network.

V. SIMULATION RESULTS AND DISCUSSION

Network simulator NS-2 version 2.34 is applied for simulation, to evaluate the functioning of the given adaptive request zone-based protocol and secure routing protocol. NS-2 allows significant Supporting almost all types of routing protocols. It comprises two tools, the ns the network simulator, which holds whole usually used IP communication protocols, and the nam is the network animator applied to project the models. Table-1shows the performance parameters used for this simulation.

TABLE I. NETWORK SIMULATION PARAMETERS

Parameter Type	Value
Simulator	NS- 2.34
X & Y dimension	1000 m x 1000 m
Channel Type	WirelessPhy
Number of Nodes	50 to 200
MAC Type (mac)	IEEE 802.11
ifq type (interface queue)	DropTail / Priqueue
ifq length	50
Antenna type	Antenna/DirAntenna
Propagation Model	TwoRayGround
Mobility Model	Random Way Point
Traffic type	CBR
Packet size	2000 bytes
Routing Protocols	AZBOSF and SAZBOSF

March - April 2020
ISSN: 0193-4120 Page No. 51 - 58

The following figures, 2 to 7 depict the simulation outcomes of these two protocols.

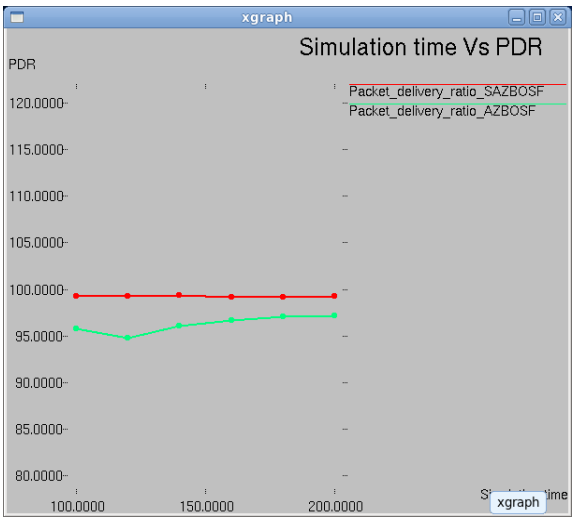

Fig.2: Comparative Analysis for Simulation time vs PDR

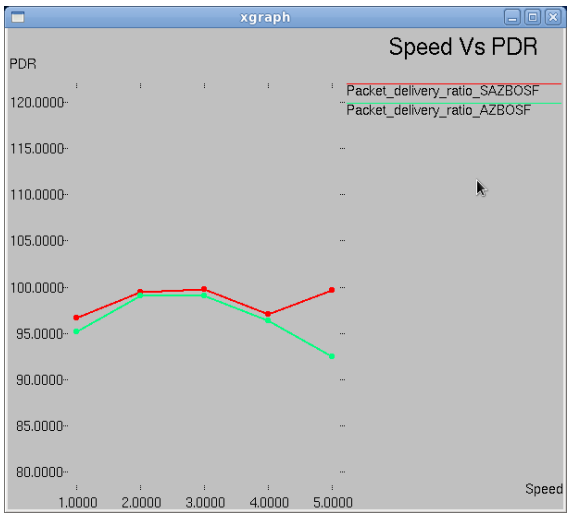

Fig.3: Comparative Analysis for Speed vs PDR

The proportional examination of the original protocol and secure protocol for a simulation time and speed versus packet delivery ratio (PDR) is depicted in figure 2 and figure 3 respectively. Results depict that the secure routing protocol's performance is better in both the scenarios.

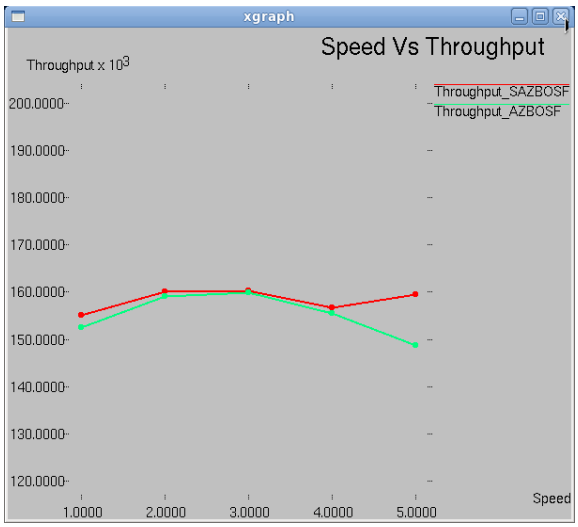

Fig.4: Comparative Analysis for Speed vs throughput

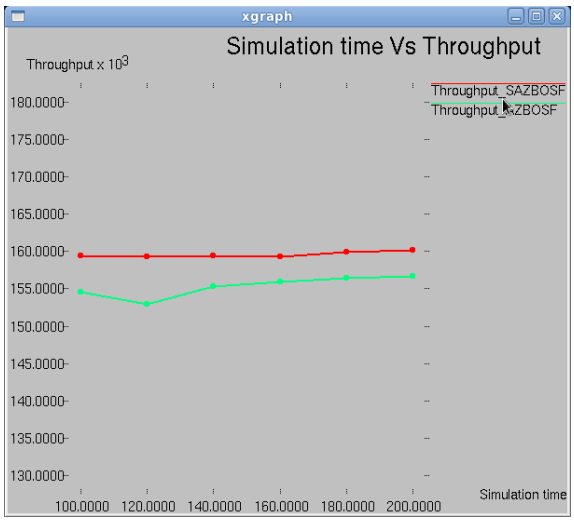

Fig.5: Comparative Analysis for Simulation time vs throughput

The comparative analysis of speed and simulation time versus throughput is depicted in Figures 4 and 5 respectively. The speed of the node varied in second from 1 sec. to 5 sec. The throughputs of the SAZBOSF protocol are higher than the AZBOSF protocol. It is noticeably understood that the performance of the MANET in terms of throughput increases after the trust with a key of the node is used.

March - April 2020
ISSN: 0193-4120 Page No. 51 - 58

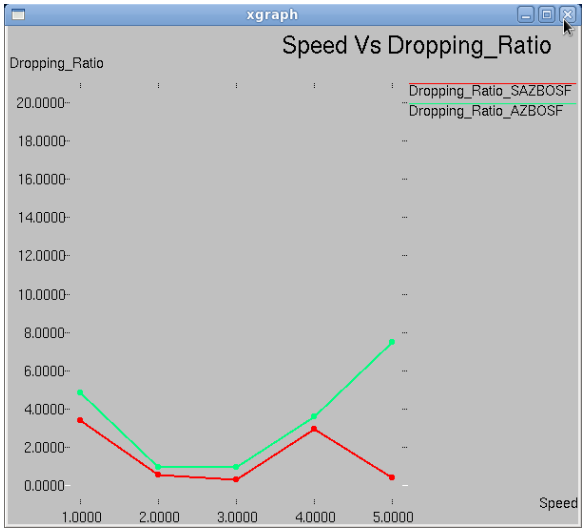

Fig.6: Comparative Analysis for Speed vs Dropping Ratio

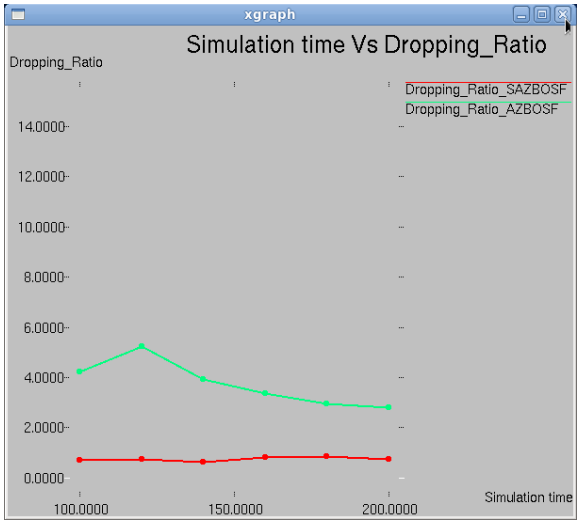

Fig.7: Comparative Analysis for Simulation Time vs Dropping Ratio

The rate of dropping ratio affects the performance of the network is well supported by the results given in Figures 6 and 7, with speed versus dropping ratio and simulation time versus dropping ratio respectively. The dropping ratio of the SAZBOSF protocol is very low compared with the AZBOSF routing protocol. The simulation time is varied from 100 seconds to 200 seconds by interval difference of 20 seconds. The performance of the secure SAZBOSF protocol is outstanding in both scenarios.

VI. CONCLUSIONS

The key management procedures are used to MANET, to accomplish the trusted transmission in this work. These procedures apply certification strategies, cryptography, certification validness for achieving protected communication in the MANET. The TF of a node is considered while issuing a certificate and authentication. The performance of the SAZBOSF routing protocol for metrics throughput, PDR and dropping ratio is excellent than the AZBOSF protocol.

This method confirms that in the MANET every node is honest and therefore safeguards the security and data integrity, and assist to a great level creating a protected network that raises the throughput and PDR and reduces the dropping ratio of the MANET. The analysis recommends improvements like the practicing of the TF of the host during selecting a node.

VII. REFERENCES

[1] G.T. Chavan and Vemuru Srikanth, "Zone Based Effective Location Aided Routing Protocol for MANET," 2nd International Joint Conference, AIM/CCPE 2012, CCIS 296, © Springer-Verlag Berlin Heidelberg 2013, pp.404–407

[2] G. T. Chavan and Vemuru Srikanth, "Zone Based Optimal Selective Forwarding (ZBOSF) Routing Protocol For MANET," PONTE International Scientific Research Journal, Vol-73, Issue 12, ISSN: 0032-423X Dec-2017, pp.339-346

[3] G. T. Chavan and Vemuru Srikanth, "Zone Based Routing Protocol with Improved Location Estimation For MANET," ARPN Journal of Engineering and Applied Sciences, Vol. 13, No. 11, ISSN -1819-6608, June-2018, pp:3650-3656

[4] Parul Tomar, P.K. Suri, and M. K. Soni, "A Comparative Study for Secure Routing in MANET," International Journal of Computer Applications (0975 – 8887), Volume 4 – No.5, July 2010, pp.17-22

[5] Ali Dorri and Seyed Reza Kamel and Esmail kheyrkhah, "Security Challenges In Mobile Ad Hoc Networks: A Survey," International Journal of Computer Science & Engineering Survey (IJCSES) Vol.6, No.1, February 2015, pp.15-29

[6] K. Vijayakumar and K. Somasundaram, " Study on Reliable and Secure Routing Protocols on MANET," Indian Journal of Science and

March - April 2020
ISSN: 0193-4120 Page No. 51 - 58

Technology, Vol -9(14), ISSN: 0974-6846, April 2016, pp: 1-10

[7] Sliman KA. A. Yaklaf, Abdurrezagh S. Elmezughi, Nasser Bashir Ekreem and Adel A. M. Abosdel, "Security Routing Protocols in Ad Hoc Networks: Challenges and Solutions," Proceedings of the International Conference on Recent Advances in Electrical Systems, Tunisia, 2016, ISBN: 978-9938-14-953-1, pp.131-135

[8] Vinay Kumar Pandey, Harvir Singh and Sanjay Kumar,"Enhanced Secure Routing Model for MANET," Computer Science & Information Technology, 10.5121/CSIT.2012.2405., 2012, pp.37-44.

[9] Panagiotis Papadimitratos and Zygmunt 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), San Antonio, TX, January 27-31, 2002, pp.1-13

[10] Panagiotis Papadimitratos and Zygmunt J. Haas, "Secure Data Transmission in Mobile Ad Hoc Networks," ACM Workshop on Wireless Security (WiSe 2003), San Diego, CA, September 19, 2003, pp. 41-50

[11] Panagiotis Papadimitratos and Zygmunt J. Haas, "Secure message transmission in mobile ad hoc networks," Ad Hoc Networks 1 (2003), pp.193–209

[12] Panagiotis Papadimitratos, "Secure Data Communication in Mobile Ad Hoc Networks," IEEE Journal on Selected Areas In Communications, Vol. 24, No. 2, February 2006, pp.343-356

[13] Yih-Chun Hu and Adrian Perrig, "Ariadne: A Secure On-Demand Routing Protocol for Ad Hoc Networks," Wireless Networks 11, Springer Science + Business Media, Inc. Manufactured in The Netherlands 2005, pp.21–38

[14] Waleed S. Alnumay and Uttam Ghosh, "Secure Routing and Data Transmission in Mobile Ad Hoc Networks ," International Journal of Computer Networks & Communications (IJCNC) Vol.6, No.1, January 2014, pp.111-127

[15] E.Suresh Babua, C Nagarajub, and MHM Krishna Prasad, "Analysis of Secure Routing Protocol for Wireless Adhoc Networks using Efficient DNA based Cryptographic Mechanism," 4th International Conference on Eco-friendly Computing and Communication Systems, ICECCS-2015, Elsevier, Procedia Computer Science 70 (2015), pp. 341 – 347

[16] P.Subbulakshmi and S.Vimal, "Secure Data Packet Transmission in MANET using Enhanced Identitybased Cryptography (EIBC)," International Journal of New Technologies in Science and Engineering Vol. 3, Issue 12,Dec 2016, ISSN 2349-0780, pp.35-48

[17] L. Raghavendar Raju and C. R. K. Reddy, "A Key Exchange Approach for Proficient and Secure Routing in Mobile Adhoc Networks," International Journal of Interactive Mobile Technologies (iJIM) – eISSN: 1865-7923, Vol-11, No-4, 2017, pp.43-54

[18] J. Vijayalakshmi and K. Prabu, " Approaches of Key Management Schemes for Mobile Ad-Hoc Networks," 3rd National Conference on Innovative Research Trends in Computer Science and Technology (NCIRCST 2018) ISSN: 2454-4248 Volume: 4 Issue: 3, March 2018, pp.4–9

[19] A. S. Khubalkar and L. R. Ragha, "Security enabled DSR for establishing symmetric key and security in MANETS," 2013 Tenth International Conference on Wireless and Optical Communications Networks (WOCN), Bhopal, IEEE-2013, pp.1-5.

[20] Vidhya P M and Ambily Mohan, " A Trust Based Routing Protocol," IOSR Journal of Computer Engineering (IOSR-JCE) e-ISSN: 2278-0661,p-ISSN: 2278-8727, pp. 79-82

[21] Jayanthi Chandrashekhar and Arun Manoharam, ' An Identity based Key Management technique for Secure Routing in MANET," International Journal of Intelligent Engineering and Systems, (IJIES), Japan, ISSN-2185-3118, 2018, pp.33-43

[22] V. Lakshman Narayana and C. R. Bharathi, "IDENTITY BASED RYPTOGRAPHY FOR MOBILE AD HOC NETWORKS," Journal of Theoretical and Applied Information Technology, Vol.95. No 5, ISSN: 1992-8645, March 2017, pp.1173-1181

[23] Jin-Hee Cho, Ing-Ray Chen, and Kevin S. Chan, " Trust threshold based public key Management in mobile ad hoc networks," Ad Hoc Networks, Elsevier, Volume 44, 1 July 2016, pp.58-75

[24] Poonam Saini and Shefali Aggarwal, "A Trust-based Uncoordinated Checkpointing Algorithm in Mobile Ad hoc Networks (MANETs)," 4th International Conference on Eco-friendly Computing and Communication Systems, Procedia Computer Science 70, Elsevier-2015, pp.311–317

March - April 2020
ISSN: 0193-4120 Page No. 51 - 58

[25] G.T. Chavan and Vemuru Srikanth, "Effective Zone Based Routing Protocols for MANET," International Journal of Advanced Trends in Computer Science and Engineering, Vol-08, No-05, ISSN 2278-3091 September-October 2019, pp.2015-2022

[26] Dragos Niculescu & B. R. Badrinath, "Ad hoc positioning system (aps)", IEEE GLOBECOM'01 (San Antonio), Nov. 2001, pp:2926-2931

[27] Lu Qingling, Bai Mengliang, Zhang Wei & Lian Enjie, "A kind of Improved DV-hop Algorithm" 2nd international conference on intelligent control and information precessing, IEEE-2011, pp:867-869

[28] Pallavi Khatri, " Using Identity and Trust with Key Management for achieving security in Ad hoc Networks," P. Khatri, "Using identity and trust with key management for achieving security in Ad hoc Networks," 2014 IEEE International Advance Computing Conference (IACC), Gurgaon, IEEE-2014, pp.271-275