Advances in Computational Sciences and Technology
ISSN 0973-6107 Volume 10, Number 4 (2017) pp. 561-574

http://www.ripublication.com

A Hybrid Aggregation Scheme for ZKP and Elliptical Curve Diffie Hellman in MANETs

[1]A.Christopher Paul and [2]Dr. S. Karthik

[1]Research Scholar, Department of Computer Science and Engineering, Karpagam University, Coimbatore, TamilNadu, India.

[2]Professor and Dean, Department of Computer Science and Engineering, SNS College of Technology, Coimbatore, TamilNadu, India.

Abstract

The mobile ad hoc networks are an independent network comprising a collection of wireless self – governing nodes communicating data among one another without any central administrator. The fundamental characteristics such as wireless medium, dynamic topology and distributed coordination are the reasons that MANETs are vulnerable to diverse security-related issues. The presence of suspicious nodes in MANETs tries to minimize the associations within the network by creating a fake synchronization thus leading to data losses. As a result, the network splits down, nodes become independent and considerably the performance of the network reduces. The hybrid scheme aggregates the better characteristics of zero knowledge protocol and elliptic curve Diffie – Hellman (ECDH) for creating a minimized route among the sender and receiver by exploring and evading the suspicious nodes from participating in between the routes. The intention is to analyze the influence of suspicious nodes within the network in terms of performance and estimate suitable assessments to identify the suspicious node for enhancing the network performance by enhancing the packet ratio, throughput and reducing delays, loads during transmission and packet losses.

I. INTRODUCTION

Mobile Ad Hoc Networks (MANETs) has become one of the most prevalent areas of research in the recent years because of the challenges it poses to the related protocols. MANET is the new emerging technology which enables users to communicate

without any physical infrastructure regardless of their geographical location, that's why it is sometimes referred to as a ―infrastructure less network. The proliferation of cheaper, small and more powerful devices make MANET a fastest growing network. An ad-hoc network is self-organizing and adaptive. The device in mobile ad hoc network should be able to detect the presence of other devices and perform necessary set up to facilitate communication and sharing of data and service. Ad hoc networking allows the devices to maintain connections to the network as well as easily adding and removing devices to and from the network. Due to nodal mobility, the network topology may change rapidly and unpredictably over time. The network is decentralized, where network organization and message delivery must be executed by the nodes themselves. Message routing is a problem in a decentralized environment where the topology fluctuates. While the shortest path from a source to a destination based on a given cost function in a static network is usually the optimal route, this concept is difficult to extend in MANET.

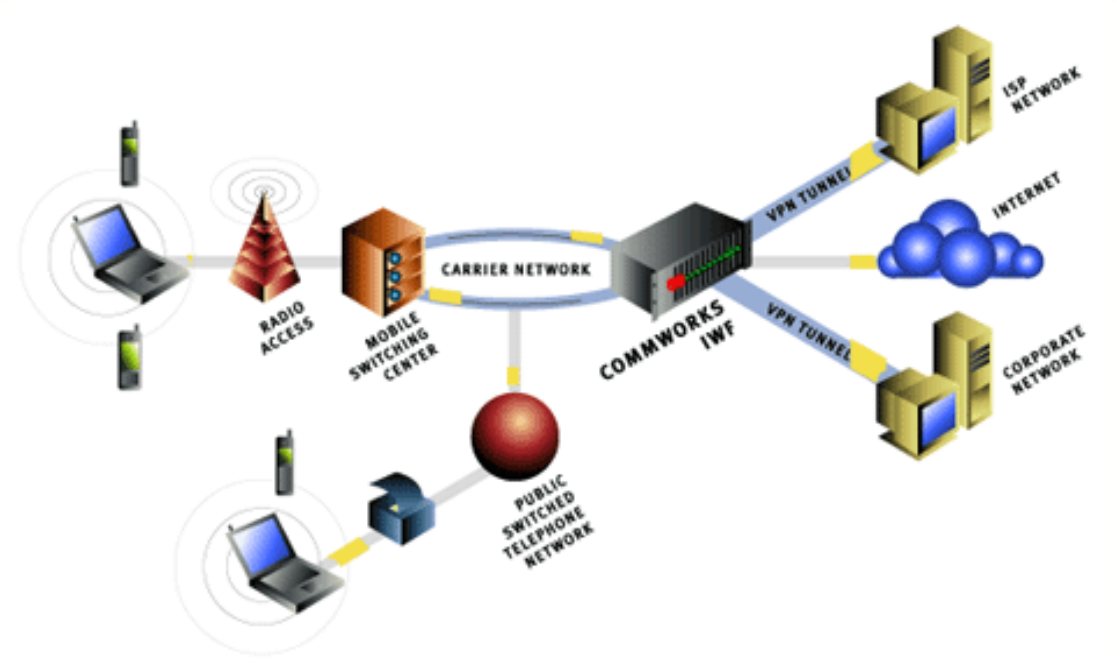

Figure 1: Infrastructure of MANET

The set of applications for MANETs is diverse, ranging from large-scale, mobile, highly dynamic networks, to small, static networks that are constrained by power sources. Besides the legacy applications that move from traditional infrastructure environment into the ad hoc context, a lot of new services can and will be generated for the new environment. MANET is more vulnerable than wired network due to mobile nodes, threats from compromised nodes inside the network, limited physical security, dynamic topology, scalability and lack of centralized management. Because of these vulnerabilities, MANET is more prone to malicious attacks.

1.1 MANET Challenges

Regardless of the attractive applications, the features of MANET introduce several challenges that must be studied carefully before a wide commercial deployment can be expected.

Routing: Since the topology of the network is constantly changing, the issue of routing packets between any pair of nodes becomes a challenging task. Most protocols should be based on reactive routing instead of proactive.

Security and Reliability: wireless link characteristics introduce reliability problems, because of the limited wireless transmission range, the broadcast nature of the wireless medium (e.g. hidden terminal problem), mobility induced packet losses, and data transmission errors.

Quality of Service (QoS): Providing different quality of service levels in a constantly changing environment will be a challenge. An adaptive QoS must be implemented over the traditional resource reservation to support the multimedia services.

Inter-networking: In addition to the communication within an ad hoc network, inter-networking between MANET and fixed networks (mainly IP-based) is often expected in many cases.

Multicasting: The multicasting is enviable to sustain multiparty wireless communications and the multicast hierarchy does not remain stable. The multicast protocols for routing should be capable enough to sustain the dynamicity within the networks which comprises the nodes also.

1.2 Assaults in MANET

The safeguarding of the wireless ad hoc networks remains a great dispute and the perception of probable assaults are always the preliminary stages towards the emergent safety related solutions. The safeguarding of communications in mobile ad hoc networks is crucial for safeguarding the communication of data within the network. These attacks can be classified into two types:

Denial of Service attack: The purpose of the assault is to bother the presence of a node or the overall network and in case the assault is thriving the services will not be offered and the intruder commonly employs wireless signal blocking and the battery depletion techniques.

Assaults in Routing: Two probable sorts of assaults are prevailing in routing. First, the assault is on routing protocol and the later is during packet transmission or during the dissemination. The initial is focused on jamming the transmission of the routing data to a node. The proceeding is focused on dissemination of packet over a fixed route.

Blackhole Attack: In this assault, the intruder broadcasts a non-value parameter to all the targets thus enabling all the nodes surrounding it to transmit the packets to it. Vulnerable node forwards false data related to routing and states that it holds the

finest path and makes other fine nodes forward the information packets using the vulnerable node. The vulnerable node plunges all the packets it acquires rather commonly acquiring these packets and the intruder snoops the requests from these flooding protocols.

Replay Attack: The intruder carries out a repeated assault over rebroadcasted legitimate information continuously for inserting it into the network traffic that has been detained earlier.

Man- in- the- middle attack: The intruder is situated between the transmitter and target and snuffles the data that is being communicated between the nodes.

II. RELATED WORKS

2.1 Proactive Protocol

In this protocol, routing information to reach all the other nodes in a network is always available in the routing table at each node. When the network topology changes, many of routes will change and update the routing table at every node which causes increasing the networks overhead. An example of proactive protocols is FSR (Fisheye State Routing) protocol

2.2 Reactive Protocol

In this protocol, discovering a route will be done just when a node wants to send data to another node in the network. When a route is discovered, it will be stored in the temporary cache at the source node until an event occurs in the network that imposes a need to new route discovering. The overhead of this protocol is less than proactive protocol. Examples of reactive protocols are DSR (Dynamic Source Routing) protocol and AODV (Ad hoc On-Demand Distance Vector) protocol.

2.3 Zero-knowledge proof protocol

A zero awareness proof or the zero awareness protocols is a scheme where the verifier can show the authenticator that the given declaration is accurate without expressing any data separately from the fact that the declaration is certainly accurate. The confirmation of the declaration necessitates awareness of some undisclosed data on the part of the verifier and the explanation entails the authenticator will not be able to confirm the declaration for anybody because the authenticator does not hold any private data.

2.4 ECDH protocol

The elliptic curve Diffie-Hellman is a secret key conformity protocol which permits the parties to hold an elliptic curve public secret key pairs for launching a distributed private through an apprehensive medium. This distributed private may be openly

employed as a key or to fetch another key which could be employed for encrypting succeeding transmission using symmetric key ciphers.

III. PROPOSED ZKP – ECDH Approach

The ECDH protocol creates a distributed key between two end parties. The actual Diffie-Hellman routine is based on the replication group modulo *p*, where the ECDH protocol is based on the additive elliptic group. Initially, the fundamental point *P*(*x*, *y*) of order n is chosen on the elliptic curve E described over the field GF(p).

The plan is to devise a verification protocol for aiding the group transmission. Nearly all the verification protocols are reliant on the ECC and employ ECDSA. The purpose is to offer an elevated level of safety by identifying the suspicious nodes. The devised protocol employs the zero awareness to validate the dynamic nodes. A zero awareness protocol is a communicative scheme for a node to confirm that the declaration is valid without enlightening the information other than the reality of the declaration.

The zero awareness protocol must assure the three features

(i) Wholeness: In case the declaration is valid the truthful authenticator will be encouraged of the information by a truthful verifier.

(ii) Accuracy: In case the declaration is not valid the fake verifier can persuade the truthful authenticator that it is valid and the fake authenticator discovers something other than the information.

(iii) Zero Awareness: In case the declaration is valid fake authenticator persuades information other than the information.

The objective of the zero awareness is to confirm the information privately without illuminating them. Every node from the cluster has a private data and each one has to confirm that it recognizes the data without illuminating them to the server. Thus, the authenticator is the consumer and the authenticator will recognize each node using an expression of their awareness. The fundamental idea of the zero awareness verification is that the authenticator inquires a query associated with the private data in a way that the reply does not possibly disclose the data.

Consider two prime numbers such as p and q where p splits (p1). Consider g be a factor of order q in pZ (the replication clusters of integers modulo p). Allow qG to be the repeated sub-cluster of order q produced by g. The integers p,q,g are identified and can be universal to a cluster of consumers. The uniqueness comprises of a secret /open pair of keys. The secret key w is an arbitrary positive integer less than q.

$$\text{The public key is estimated as} \quad Y=g^{-w} \bmod p \tag{1}$$

The protocol is described as below Common Input: p,q,g,y; A safety metric t. Safety Input for an authenticator: $w \epsilon Z_q$ such that $Y=g^{-w} \bmod p$

1. Assurance by the authenticator, authenticator picks , $r \epsilon Z_q$ compute $x=g^r \bmod p$ and transmits it to the verifier.

$$\text{Prover} \xrightarrow{x = g^r} \text{Verifier}$$

2. Dispute from authenticator, authenticator chooses a number $e \epsilon [1\ 2^t]$ and forwards it to the authenticator

$$\text{Prover} \xrightarrow{e} \text{Verifier}$$

3. Reply from authenticator, authenticator estimates $s=(r + w.e) \bmod q$ and forwards it to the validator

$$\text{Prover} \xrightarrow{s=r+w.e} \text{Verifier}$$

The validator ensures $x=g^s y^e \bmod p$ and understands if and only if parity sustains and it is well recognized that the Schnorr's protocol is a truthful authenticator zero awareness protocol of awareness of the separate logarithm of y. The Schnorr's protocol is based on the elliptic curve and is entailed as below.

Procedure

Let p and q be the prime numbers

p divides p1

g is a factor of order q in pZ

$Y=g^{-w} \bmod p$ is the public key

Input : p,q,g,y

Include 't' as security parameter

$w \epsilon Z_q$ serves as authenticator

Employ $r \epsilon Z_q$ to estimate $x=g^r \bmod p$

Authenticator selects $e \epsilon [1\ 2^t]$

After reply authenticator estimates $s=(r + w.e) \bmod q$

Forward to validator

validator performs $x=g^s y^e \bmod p$

Consider a point on the elliptic curve entailed over a restricted field of order, then,

(i) If α is the authenticator's private data then consumer makes open $Z=\alpha P$.
(ii) The authenticator selects an arbitrary number r and forwards $X=rP$ to the validator

(iii) The validator selects an arbitrary number e and forwards it to the authenticator.
(iv) The authenticator estimates $Y=(\alpha e+r) \bmod n$ and forwards it to the validator.
(v) The target receives y and accepts if $yP+eZ=X$.

Soon after the authentication process by the originator and the target the transmission begins between the verified consumers within the network. The entire dynamic node utilizes the similar key pairs (P (public key), S (private key)) since all these possess to recognize the messages forwarded from any nodes of the cluster. These key pairs along with the server are employed for transmission during every schedule. Two nodes cannot transmit using this protocol without the awareness of the rest. If a node acquires a message it can be sniffed by rest of the nodes because it is possible for decryption. Additionally, a key for a node is initiated by an attacker all the nodes are exaggerated. The level of safety can be elevated using a point P (secret) on elliptic curve E. The public metrics are the prime number p and a, b entailing the elliptic curve $E_p(a,b)$ in a way $y^2=x^3+ax+b$ with $\gcd(4a^3+27b^2, p)=1$. The RSA routine is employed to create the key pair (e,d).

If A and B are the two transmitting parties then the routine is entailed as below.

i. A chooses two arbitrary numbers X_A, R_A in E_p and a point P_A on elliptic curve.
ii. B chooses two arbitrary numbers X_B, R_B in E_P and a point P_B on an elliptic curve.
iii. A forwards $G_A=X_AP_A$ to B.
iv. B forwards $G_B=X_BP_B$ to A .
v. A forwards $S_A=R_AG_B$ to B.
vi. B forwards $S_B=R_BG_A$ to A.
vii. A estimates the scheduled key *P*ub = $e(S_A + S_B)$.
viii. B estimates the scheduled key *P*ub = $e(S_A+S_B)$.
ix. The secret key will be Sec = $d(S_A + S_B)$.

IV. PERFORMANCE ANALYSIS AND RESULTS

4.1 Mobility of the Network

4.1.1 Mobility vs. Packet Delivery Ratio

Figure 1, conducts a performance comparison between the AODV and Hybrid approach (ZKP+ECDH). Here we investigate on the packet delivery ratio of AODV and modified routing protocol ZKP + ECDH for different node mobility. The hybrid approach protocol (ECDH+ZKP) estimate path for packet delivery and assures the packets are disseminated to the proper target through trustworthy intermediate nodes.

From figure 1, it is observed that AODV & Hybrid approach (ECDH+ZKP) always performs better in terms of PDR and Mobility. It is also seen that the packet delivery ratio decreases whenever the mobility increases. This is due to frequent change in topology, which leads to frequent path break and packet loss. However, the proposed hybrid approach outperforms AODV in all mobility speeds.

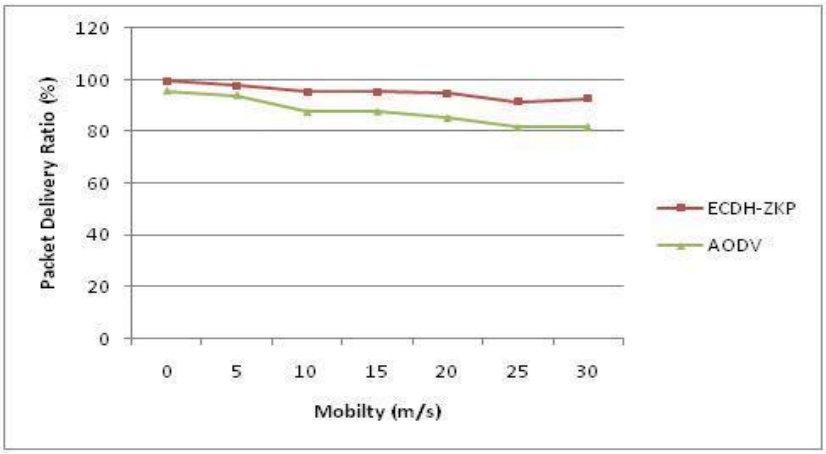

Figure 2: Mobility vs. Packet Deliver Ratio

4.1.2 Mobility Vs Routing Load

ECDH+ZKP protocol has significantly low routing overhead than AODV when the mobility is increased. The results show that when the number of sources is low the performance of ECDH+ZKP and AODV is similar regardless of mobility.But with a large number of sources ECDH+ZKP starts outperforming AODV for high mobility scenario. Further, ECDH+ZKP always have a lower routing overhead than AODV. In ECDH+ZKP route replies contribute to large fraction of routing overhead and assures that communication in held with trustworthy nodes in network

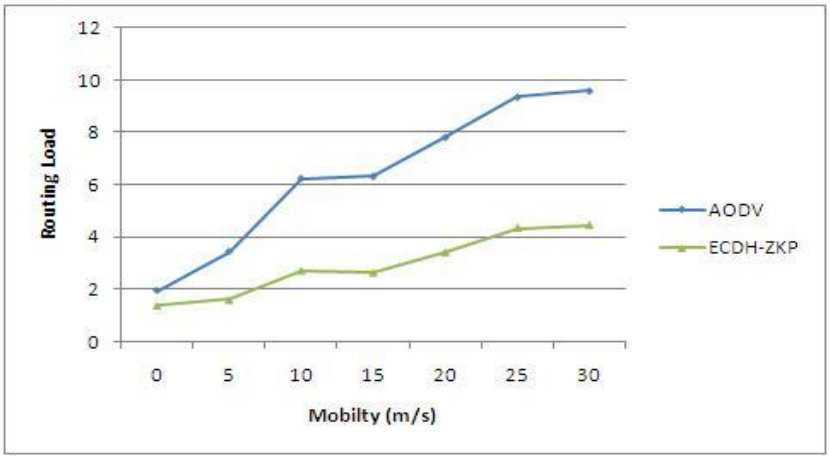

Figure 3: Mobility vs. Routing Load

4.1.3 Mobility Vs Average Delay

From Figure3, Average end–end delay of ECDH+ZKP is comparable to AODV when there is low mobility in the network, but with the increased mobility in the network, delay in AODV is too much higher than ECDH+ZKP. ECDH+ZKP perform better in all condition. Overall in case of real-time packet delivery, ECDH+ZKP is a better choice. AODV produce more delay due to route caching and malicious node in the network. ECDH+ZKP establish a shortest path between sender and receiver by identifying and avoiding the malicious node to participate in the path. Average end-end delay in case of AODV traffic is at least three times more than ECDH+ZKP traffic.

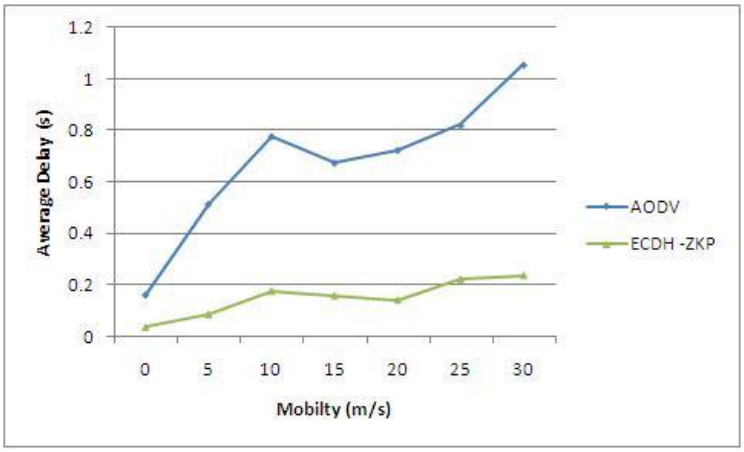

Figure 4: Mobility vs. Average Delay

When the mobility increases the packet loss also increases which increases in congestion. This is because; the probability of route breaking is frequently increased when the mobility increases. This will increase the number of route request packet and leads to congestion. The congestion again increases the loss of packets. However, hybrid approach performs better in all mobility speeds

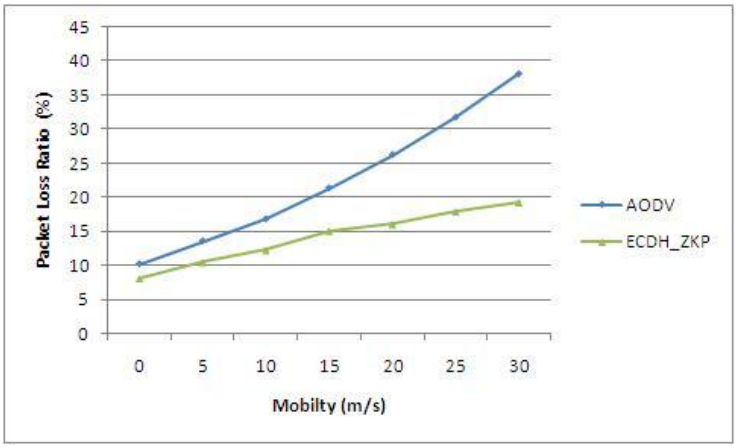

Figure 5: Packet Loss ratio vs. Mobility

4.1.5 Mobility vs. Network Throughput

AODVwith ECDH+ZKP show higher throughput than AODV. The throughput of AODV, with different mobility models, decrease when increasing the density of nodes. But, with AODV ECDH+ZKP produce high throughput. The Figure5 shows that ECDH+ZKP has maximum throughput than AODV.

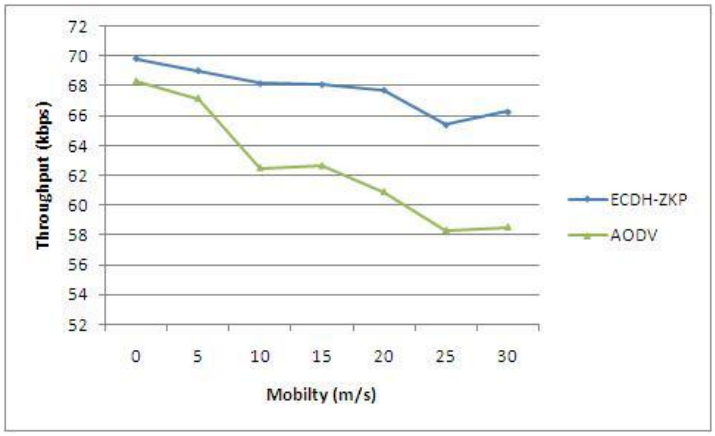

Figure 6: Throughput vs. Mobility

4.2 Numbers of Malicious Nodes

4.2.1 Number of malicious Node Vs Average Delay

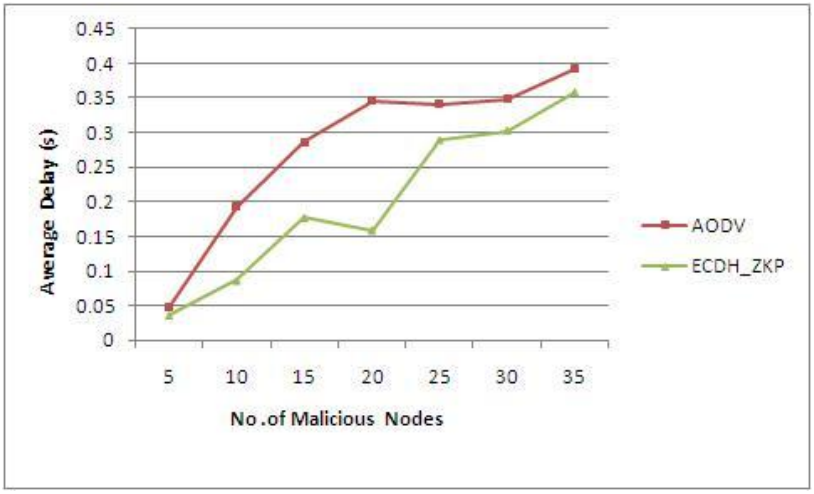

Figure7: Average Delay vs. No. of malicious nodes

The malicious nodes are acting selfishly and denied to forwarding the packet to its neighbors. Due to this nature, the time taken for transmission of the packet is increased. Hence, the delay also increased. However, hybrid approach performs better

than AODV since this approach identifying those malicious nodes and eliminates while forwarding the packet. By having the route which didn't have malicious node the hybrid approach attains better results in all variations on malicious nodes.

4.2.2 Number of malicious Node Vs Routing Overhead

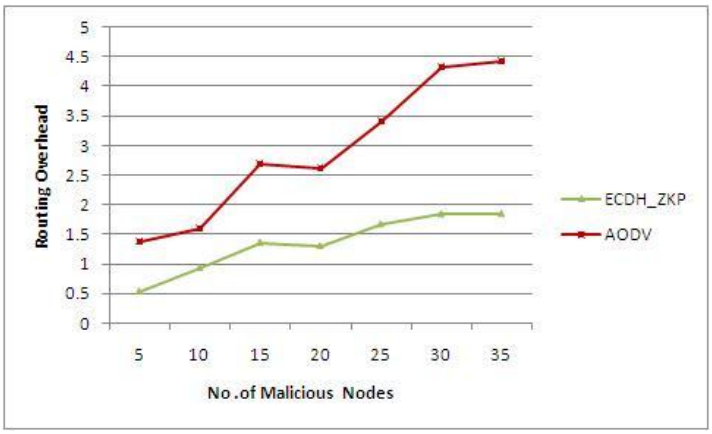

Figure 8: Routing Overhead vs. No. of malicious nodes

When the number of a malicious node increases the denial of packet forwarding also increased. Hence the sender has to go for choosing a new route by considering the existing route as a stale route. This scenario increases the number of route request packet in the network and leads to higher overhead in routing. Figure 7 shows the performance of AODV and hybrid approach. In this, by combining the best features of ECDH and ZKP this approach identify and eliminate the kind of stale routes during the route discovery process. Hence it shows the improved performance while comparing with AODV.

4.2.3 Number of malicious Node Vs Packet Delivery Ratio

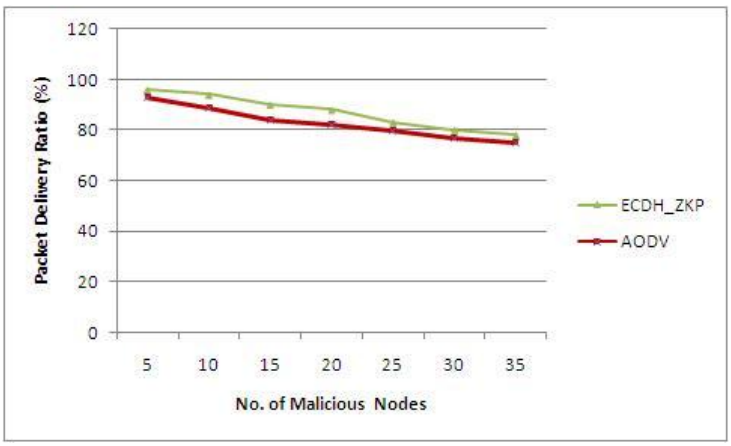

Figure 9: Packet Deliver Ratio vs. No. of malicious nodes

The figure8 shows the performance comparison of AODV and hybrid approach with respect to the successful delivery of packets. In the figure, the delivery ratio linearly decreases while increasing the number of malicious nodes. While avoiding the stale route in a hybrid approach, the network is unfortunate to losses number of routes to the destination. When the network has less number of routes the contention also high among the nodes. This will lead to loss of packets and retransmission of lost packets.

4.2.4 Number of malicious Node Vs Packet Loss Ratio

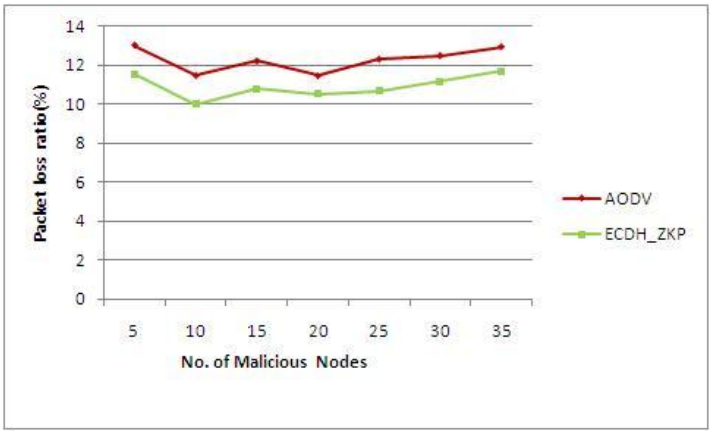

Figure 10: Packet loss ratio vs. No. of malicious nodes

Due to stale routes in the network, the number of packets lost in the network also increased linearly in both approaches. The figure9 show the performance comparison of AODV and hybrid approach. However, hybrid approach performs better than the AODV

4.2.5 Number of malicious Node Vs Average Throughput

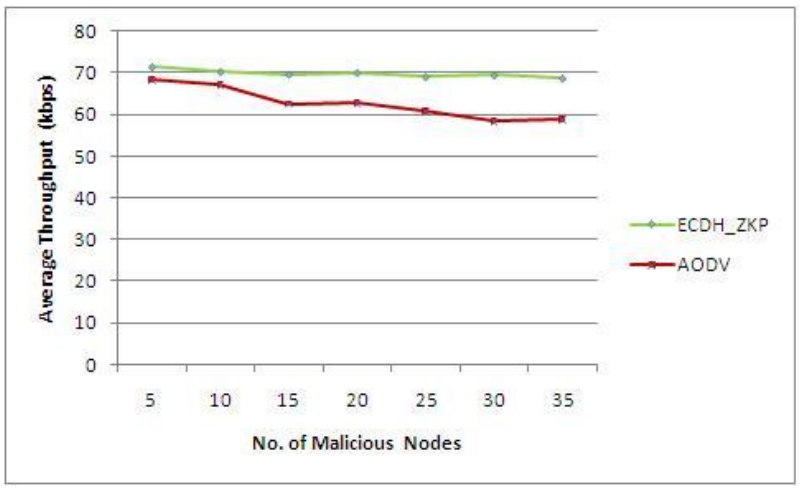

Figure11: Average Throughput vs. No. of malicious nodes

The throughput of the network increases or remains same when no. of malicious in the network increases. Figure10 demonstrates the comparison between the performance of AODV and Hybrid approach. In both approaches, the throughput linearly decreases. However, the hybrid approach maintains the better level of throughput in all cases of a number of malicious nodes. This could be possible by the hybrid approach because it avoids the as possible as much of malicious nodes while establishing the routes to the destination. Even though there is a possibility of having less number of routes.

V. CONCLUSION

The major focus of this paper is to design an enhanced approach by combining the best features of zero knowledge protocol and Elliptic curve Diffie–Hellman algorithms to detect and eliminate the malicious nodes which will degrade the performance mobile Adhoc network. In the signing phase of the ZKP, the mobile nodes are restricted to share the secret information between them. Due to this restriction, no information about the mobile nodes is shared between each other. This will make the signing process as week one. To enhance this, in the proposed work we extract the concept of verification and key generation process used in ECDH. Here, the prover and verifier share the self-generated random numbers among them and by making the secret information as public. The receiver node accepts and receives the computed secret message when that message matches with the preconditions. Where the precondition is made by combing random numbers. To analyze the performance of new approach the results are compared against by varying the node mobility and number of malicious node in the network. Network throughput, packet delivery ratio, routing overhead, average delay and packet loss ratio are considered Quality of service parameters in this analysis. In the results, the performance of ECDH-ZKP is compared against malicious AODV and the results are proved that ECDH-ZKP is performed better in all the considered circumstances than malicious AODV.

REFERENCES

[1] Takuji Tsuda, Yuka Komai, Takahiro Hara, (Senior Member, IEEE), and Shojiro Nishio, (Fellow, IEEE), top-k query processing and malicious node identification based on node, march 14, 2016

[2] S. Chen, Y. Zhang, Q. Liu, and J. Feng, ``Dealing with dishonest recommendation: The trials in reputation management court," Ad Hoc Netw., vol. 10, no. 8, pp. 1603_1618, Nov. 2012.

[3] Laurent Yamen Njilla, Patricia Echual, Niki Pissinou3, Kia Makki, A Game-Theoretic Approach on Resource Allocation With Colluding Nodes in MANETs Grouping in manets, IEEE ,978-1-4673-9519-9/16/$31.00 ©2016

[4] L. Yamen Njilla, N. Pissinou, “Dynamics of Data Delivery in Mobile Ad-hoc networks: A Bargaining Game Approach”, IEEE Computational Intelligence

and Security in Defense Applications (CISDA), pp: 1-6, Verona, NY, USA, May 2015.

[5] R. Myerson "Game Theory: Analysis of Conflict" Harvard University Press, 1997

[6] L. Buttyan, J-P Hubaux, "Stimulating Cooperation in Self-Organizing Mobile Ad Hoc Networks", ACM/Kluwer Mobile Networks and Applications, 8(5), October 2003.

[7] Y. Liou, R. Gau, C. Chang, "A bargaining game based access network selection scheme for HetNet", Proc. IEEE International Conf. on Communications, pp: 4888-4893, Sydney, Australia, June 2014.

[8] Lindell,Y;Zarosim,H.Adaptive Zero-knowledge Proofs and Adaptively Secure Oblivious Transfer.[J].Journal of Cryptology.24(4),pp.761-799,2011

[9] M. Aydos, B. Sunar and C. K. Koc, An Elliptic Curve Cryptography based Authentication and Key Agreement Protocol for Wireless Communication, Proceedings of the 2nd International Workshop on Discrete Algorithms and Methods for Mobile Computing and Communications, Dallas (1998),

[10] R. Zhang, L. Cai, and J. Pan, "Performance study of hybrid MAC using soft reservation for wireless networks," in Proc. IEEE ICC'11, 2011,pp. 1–5.

[11] M. Natkaniec, K. Kosek-Szott, S. Szott, J. Gozdecki, A. Głowacz, and S. Sargento, "Supporting QoS in integrated ad-hoc networks," Wireless Pers. Commun., vol. 56, no. 2, pp. 183–206, 2011.

[12] A. Abdrabou and W. Zhuang, "Stochastic delay guarantees and statistical call admission control for IEEE 802.11 single-hop ad hoc networks," IEEE Trans. Wireless Commun., vol. 7, no. 10, pp. 3972–3981, 2008.

[13] S. Jiang, J. Rao, D. He, X. Ling, and C. C. Ko, "A simple distributed PRMA for MANETs," IEEE Trans. Veh. Technol., vol. 51, no. 2, pp. 293–305, 2002.

[14] K. Medepalli and F. Tobagi, "System centric and user centric queueing models for IEEE 802.11 based wireless LANs," in Proc. IEEE Broad-Nets'05, 2005, pp. 612–621.

[15] L. Kleinrock and F. Tobagi, "Packet switching in radio channels: Part I–carrier sense multiple-access modes and their throughput-delay characteristics," IEEE Trans. Commun., vol. 23, no. 12, pp. 1400–1416, 1975.

[16] A. Abdrabou and W. Zhuang, "Service time approximation in IEEE 802.11 single-hop ad hoc networks," IEEE Trans. Wireless Commun., vol. 7, no. 1, pp. 305–313, 2008.