Enhanced AODV with Secrete Key Sharing to Improve Security and Energy Efficiency in MANETs

Mr. Murali G [#1], Ms. Divyashree B.N [#2], Dr. Balakrishna R [#3], [#4]Dr M.Vinayaka Murthy
[#1] *Research Scholar, Reva University,*
Associate Professor, Department of Information Science and Engineering
SJB Institute of Technology, 560060, Karnataka, India
[#2] *PG Scholar, CNE, Dept. of ISE*
SJB Institute of Technology, 560060, Karnataka, India
[#3]*Principal and Professor*
Raja Rajeshwari College of Engineering Bangalore -560074, Karnataka, India
[#4] *Professor*
School of Computer Science and Application, Reva University.

ABSTRACT: Mobile Ad-hoc Networks (MANET) is one of the most important emerging research areas in the world. MANET nodes are miniature devices with limited energy, memory, transmission range, and computational power. Protecting the networks from different kinds of attacks i.e, security in wireless ad-hoc networks plays a decisive role and has received increased consideration in the current generation. As the goal of the MANET is to gather data from the deployed ad-hoc nodes and in-network processing, or data aggregation, the research.community are mainly concentrating in providing energy efficient paths in the network. Many protocols have been proposed in MANETs to provide security and energy efficiency. In this paper, by using Ant Colony Optimisation approach in AODV, the best energy efficient paths in the network are obtained. As nodes are portable in nature securing the network is also the main aim of the paper. The key distribution technique is used to aggregate and maintain the secrecy of data. The elliptic curve cryptography (ECC) data aggregation will enable the intermediate nodes for key distribution and key authentication.

Keywords— MANET, Data Aggregation, Elliptic Curve Cryptography, Ant Colony Optimization.

I. INTRODUCTION

A MANET is a network consisting of numerous wireless nodes, which work together in determining some sort of physical or environmental conditions, such as temperature, sound, vibrations, light, movement etc. The individual ad-hoc nodes are small and have inadequate energy, computational power and memory which puts some fetters on the applications and protocols which are designed for use in such networks.

As these wireless ad-hoc nodes are tiny devices with restricted energy, reminiscence, transmission range, and computational power, a cluster head is usually used in the network, which receives the data from the nodes. Such a cluster head is usually a dominant computer with more computational power, energy and memory. These cluster heads can also be misinterpreted by the attackers. Therefore, some amount of security is required in order to maintain high survivability and reliability of the network.

Several nodes may be tasked with determining the phenomenon of collecting data, these nodes may cooperate in a ―cluster‖ where one node is tasked with compressing the result from all the other nodes in the cluster and produce a ―collective view‖ of the cluster on the situation, which is called as data aggregation. Because of the nature of wireless ad-hoc networks, all nodes in the network may not have a direct association with other nodes in the network. Hence, they make use of multi-hop communication in order to communicate. Multi-hop communication in wireless ad-hoc networks is expected to consume less power than the traditional single hop communication, which is also enviable in order to keep the communication costs at its minimum.

Ad-hocs are often deployed in easily reached areas, which add the risk of physical attack. This is why wireless ad-hoc networks pose inimitable challenges. Attacks can be internal or external kind. The attacker can be either active or passive. There are different attacker types which are considered in the paper is black hole attack. The black hole is a node which acts as a normal node by advertising the path to destination but discards all the packets it receives.

By minimizing delay in packets delivery, the life time of the network and Quality of Service of the network can be improved, which can also be extended by using suitable energy efficient routing protocol.

The design of a Wireless Ad-hoc Network depends on the application, and it must deliberate factors such as the environment, the application‘s design objectives, and system constraints.

II. Related Works

Several energy aware routing protocols are designed based ACO heuristics. Gupta et al[1] did a comparison of three ACO-based protocols : Ant-AODV, Ant-DSR and Ant-DYMO based on different performance metrics like routing overhead, end-to-end delay and few other many. Radwan et al [2] proposed AntNet RLSR, in which mobile agents build routes between source and destination simultaneously discovering network activities and updating routing table. Zhu et al. [3], for asymmetric schemes focused on preserving data integrity and proposed an efficient integrity-preserving data aggregation protocol named EIPDAP. The scheme is based on the modulo addition operation using ECC, and has the most optimal upper bound on solving the integrity-preserving problem for data aggregation. Niu et al. [4] proposed a secure identity-based lossy data aggregation scheme using homomorphic hashing and identity-based aggregate signature. In the scheme, the authenticity of aggregated data can be verified by both aggregators and BS. The computation and communication overheads could be significantly reduced because the BS can perform batch verification. However, the above two schemes may lead to the leakage of data privacy due to decryption at the aggregator.

West off et al. [5] Based on PH, proposed CDA methods to facilitate aggregation in encrypted data, where richer algebraic operations can be directly executed on encrypted data by aggregators.

Mykletun et al. [6] adopted several public-key-based PH encryptions to achieve data concealment in WSNs. Furthermore. Girao et al. [7] proposed a novel scheme by extending the EL Gamal PH encryption.

III. Proposed System

In this section, Architecture of the proposed system is explained. It includes Network Initialization, Cluster formation, Key distribution, E-AODV routing, Data Aggregation and Data Authentication.

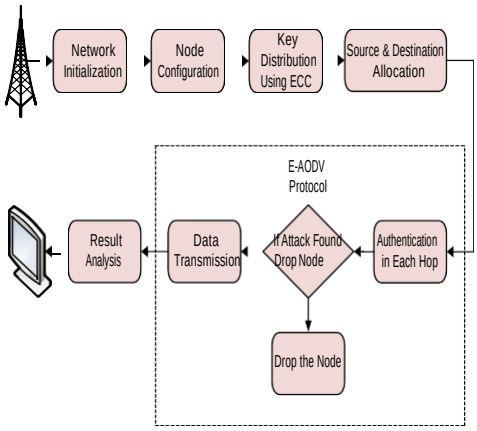

Figure 1.Block Diagram of Proposed System.

a. *Data Aggregation*

Data aggregation is one of the techniques to effectively utilize the limited resources. Generally it consists of the following steps :(i) Cluster head selection(ii) Cluster group formation. (iii) Transfer of data. There are few protocols that can perform the data aggregation and routing simultaneously. In each cluster, cluster head is chosen to collect the data from all the ad-hoc nodes and aggregate and send it to the requested base station depending on the energy of each node. Here we make use of a LEACH-KED[3] algorithm to form the clusters. Once clusters are formed, data aggregation process will begin. Then the data will be transmitted to the destination securely using ant colony optimised demand routing protocol Ad-hoc on-Demand Distance Vector (E-AODV) for a secure hop-by-hop data aggregation. In this, data is encrypted by the transferring nodes and decrypted by the aggregator nodes which then aggregate the data and encrypt the aggregation result again. At last the sink node gets the final encrypted aggregation data and decrypts it. Aggregate nodes are vulnerable to attack because of decryption of the ad-hoc data‘s in it.

b. *Ant Colony Optimization in AODV*

Ant Colony Optimization (ACO) is the foraging behaviour of real ants that tries to find the shortest paths between food sources and the nest which is helpfull in finding the optimised paths to the destination. The ACO's amalgamation is also motivated by the usual good performance shown by the algorithms using it. The ACO in AODV works as follows:

1. The route discovery phase is initiated when the source node initiates to send message

across the network by broadcasting the route request packet which are forwarded to the neighbouring nodes in the network. These neighbour nodes forward the request packet to their nodes till the destination node is reached.

2. Nodes while forwarding the route request packet checks for the residual energy of the neighbouring nodes and select for the routing path in the network.
3. As the nodes lose energy, those nodes will be dropped and the alternative nodes with high residual energy will be selected for routing.
4. After the route request packet reaches the destination, authentication part is done and the route reply packet is generated and traversed back to the source node.
5. After the source node receives the route reply packet from the destination, the source node records the path in the table. If the source node receives multiple route replies, the route with optimized path is selected for data transmission.

If any link failure occurs in the network during data transmission, the route error packet is generated and transmitted source node and an alternative path for destination is done. The energy of the nodes are determined by the below formula

If((Node N< 0.9* E_avg)

then(drop RREQ)) , (1)

The nodes that satisfies the above condition are considered during data transmission. The nodes that do not have sufficient energy are discarded until and unless they possess the required amount of residual energy for the capability of transmission.

c. Data Authentication

It is the confirmation of sender or receiver. It ensures that communicating node is the one that it has to communicate with.

In this paper, using Elliptic Curve Cryptography (ECC) which is an approach to public-key cryptography that is based on the algebraic structure of elliptic curves over fixed fields. Public-key cryptography is based on the intractability of firm mathematical problems. Earlier public key systems, such as RSA algorithm, are secure assuming that its difficult to factor a large integer composed of two or more large prime factors. For elliptic-curve-based protocols, it is believed that finding the discrete logarithm of a random elliptic curve element with respect to a publicly-known base point is infeasible. The size of the elliptic curve determines the complexity of the problem. It is believed that, the level of security afforded by an RSA-based system with a large modulus can be achieved with a much smaller elliptic curve group by using a small group that reduces storage and transmission requirements.

SP-ECC Message Authentication: In this section, we propose an absolutely secure and efficient SP-ECC. The main idea is that for each message m to be unconfined, the message sender, or the sending node, generates a source unnamed message authenticator for the message m. The generation is based on the MES scheme on elliptic curves. For a ring signature, each ring member is required to compute a forgery signature for all other members in the AS. In our scheme, the entire SP Massage authentication generation requires only three steps, which link all non-senders and the message sender to the SP alike. In addition, our design enables the SP-ECC message authentication to be verified through a single equation without individually verifying the signatures.

Let p > 3 be an odd prime. An elliptic curve E is defined by an equation of the form:

$$E: y^2 = x^3 + ax + b mod p, \quad (2)$$

Where $a, b \in F_p$, and $4a^3 + 27b^2 \neq 0 mod p$. The set $E(F_p)$ consists of all points $(x, y) \in F_p$ on the curve, together with a special point Q called the point of infinity.

Let $G = (x_G, y_G)$ be a base point on $E(F_p)$ whose order is a very large value N. User A selects a random integer $d_A \in [1, N-1]$ as his private key. Them, he can complete his public key Q_A from $Q_A = d_A \times G$.

Signature generation algorithm as follows.

Step1: select a random integer k_A, $1 \leq k_A \leq N-1$.

Step2: Calculate $r = x_A mod N$, where $(x_A, y_A) = k_A G$. If r=0, go back to step 1.

Step3: Calculate . If r=0, go back to step 1.

Step3: Calculate $h_A \overleftarrow{l} h(m,r)$, where h is a cryptographic has function, such as SHA-1, and $\overleftarrow{l}$ denotes the l leftmost bits of the hash.

Step4: Estimate $s = rd_A h_A + k_A mod N$. If s=0, go back to step 2.

Step5: the signature is the pair (r,s).

Signature Verification algorithm is as follows:

Lets say for Sender authenticate the receiver signature, the receiver must have the public key Q_A, then the algorithm steps follows as shown below.

Step1: Checks that $Q_A \neq 0$, otherwise invalid

Step2: Checks that Q_A lies on the curve.

Step3: Checks that $nQ_A = 0$

d. Attack Model

Black hole attack this is a DoS attack, where a malicious node advertises a zero cost route through itself. If the routing protocol in the network is a –low cost route first‖ protocol, like distance vector, other nodes will chose this node as an intermediate node in routing paths. The neighbours of this node will also chose this node in routes, and compete for the bandwidth. This way the malicious node creates a black hole inside the networks.

IV. RESULTS

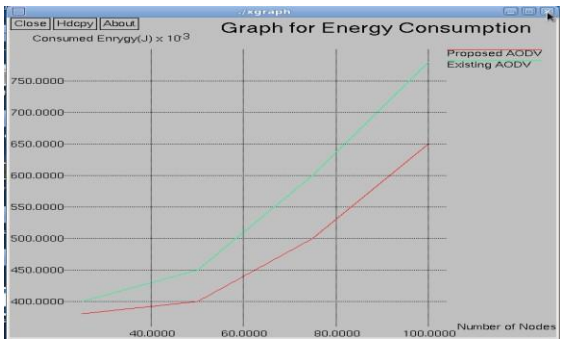

Figure 2: Energy Consumption as the number of nodes increases.

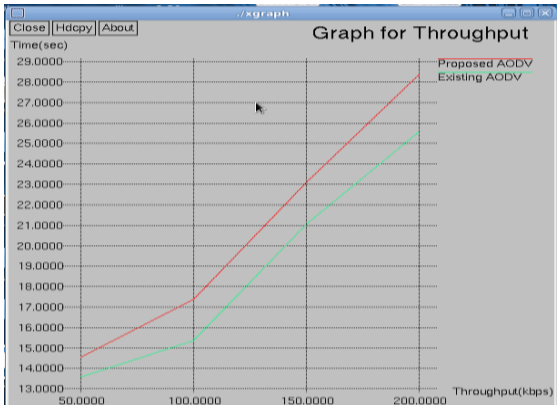

Figure 3: Throughput

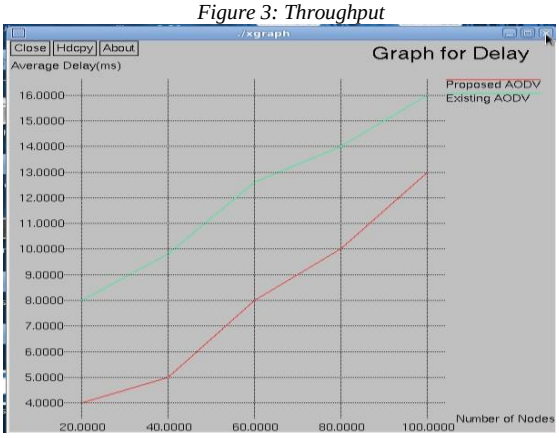

Figure 4: Delay.

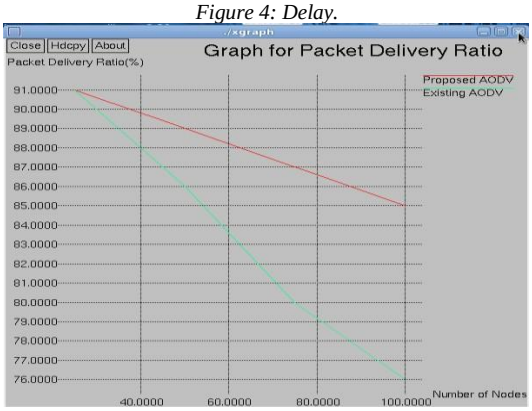

Figure 5: Packet Delivery Ratio.

V. CONCLUSION

The main Objective of the proposed system is to increase the network lifetime by reducing the energy consumption of ad-hoc nodes during data transmission. In this paper, ant colony optimization with AODV as well as encrypted-data aggregation scheme based on elliptic curve cryptography that exploits a smaller key size are proposed. Additionally, it allows the use of higher number of operations on cipher-texts and prevents the distinction between two identical texts from their cryptograms. These properties permit the approach to achieve

higher security levels than existing cryptosystems in ad-hoc networks. Performance evaluation shows the proposed system works much better than existing system in terms of energy consumption, throughput, delay and packet delivery ratio.

References

[1] A. K. Gupta, H. Sadawarti and A. K. Verma, ―MANET Routing Protocols Based on Ant Colony Optimization‖, Intl. Journal of Modelling and Optimisation, vol 2, pp. 42-49, feb 2012.

[2] A. A. Radwan, T. M. Mahmoud and E. H. Hussein, ―AntNet-RSLR: A proposed Ant Routing protocol for Manets‖, Proc, of IEEE Saudi Intl. Electronics, communication and Photonics Conference Riyadh, Saudi Arabia, pp 1-6, Apr 2011.

[3] Zhu et.al[1], ― An Efficient data aggregation protocol concentrated on data integrity in wireless ad-hoc networks.‖ Int. J. Distrib. Sens. Netw. 2013, 2013, 256852.

[4] Niu, et.al[2] ―Lossy data aggregation integrity scheme in wireless ad-hoc networks.‖ Comput. Electr. Eng. 2013, 39, 1726–1735.

[5] Westhoff,et.al[3],‖ Concealed data aggregation for reverse multicast traffic in ad-hoc networks: Encryption, key distribution, and routing adaptation‖. IEEE Trans. Mob. Comput. 2006, 5, 1417–1431.

[6] Mykletun, E.; Girao, J.; Westhoff, D. Public key based cryptoschemes for data concealment in wireless ad-hoc networks. In Proceedings of the IEEE International Conference on Communications (IEEE ICC ‘06), Istanbul, Turkey, 11–15 June 2006; pp. 2288–2295.

[7] F. Ye, H. Lou, S. Lu, and L. Zhang, ―Statistical En-Route Filtering of Injected False Data in Ad-hoc Networks,‖ Proc. IEEE INFOCOM, Mar. 2004.

[8] S. Zhu, S. Setia, S. Jajodia, and P. Ning, ―An Interleaved Hop-By-Hop Authentication Scheme for Filtering False Data in Ad-hoc Networks,‖ Proc. IEEE Symp. Security and Privacy, 2004.

[9] M. Albrecht, C. Gentry, S. Halevi, and J. Katz, ―Attacking Cryptographic Schemes Based on ‗Perturbation Polynomials‘,‖ 2009.

[10] Lejla Batina, Nele Mentens, Kazuo Sakiyama, Bart Preneel, and Ingrid Verbauwhede, ―Low-Cost Elliptic Curve Cryptography for Wireless Ad-hoc Networks‖, Springer, pp. 6–17, 2006.

[11] Sweta Nigam and K.N. Hande, ―Survey on ―Security Architecture Based on ECC (Elliptic Curve Cryptography) in Network‖, International Journal of Computer Science and Mobile Applications, Volume 3, Issue 1, 2015.

[12] Mehala.G and Mariselvi.J, ―Source Anonymous Message Authentication in Security Networks‖, International Journal of Computer Trends and Technology, volume 17, Issue 3, 2014.

[13] Chinnaswamy C.N and Natesha B V, ―Message Authentication between the Nodes using modified El-Gamal Signature on Elliptic Curve‖, International Journal for Advance Research in Engineering and Technology, Volume 2, Issue V, 2014.

[14] Naipunya H C, Nalina G R, Gururaj H L and Ramesh B, ―Secured Source Anonymous Message Authentication Using Wireless Ad-hoc Network‖, Journal of Computer Engineering, Volume 17, Issue 3, 2015.

[15] I.F. Akyildiz, W. Su, Y. Sankarasubramaniam, E. Cayirci, A survey on ad-hoc networks, IEEE Commun. Mag. 40 (8) (2002) 102–114. [2] J. Yick, B. Mukherjee, D. Ghosal, Wireless ad-hoc network survey,Comput. Networks 52 (12) (2008) 2292–2330. [3] K. Akkaya, M. Demirbas, R.S. Aygun, The Impact of Data Aggregation on the Performance of Wireless Ad-hoc Networks, Wiley Wireless Commun. Mobile Comput. (WCMC) J. 8 (2008) 171–193.

[16] Girao, J.; Westhoff, D.; Mykletun, E.; Araki, T. TinyPEDS: Tiny persistent encrypted data storage in asynchronous wireless ad-hoc networks. Ad Hoc Netw. 2007, 5, 1073–1089.