Implementation of Hybrid Cryptography in WSN with analysis and comparison of its performance in AODV, DSDV and ZRP routing protocols

[1]Zuhi Subedar, [2]Ashwini Araballi

Jain College of Engineering,
Belagavi, Karnataka, India

***Abstract*: The use of wireless network is increasing on a rapid pace because of the various advantages offered by these networks. These networks include mobile ad hoc networks (MANETs), vehicular ad hoc networks (VANETs), wireless sensor networks (WSNs) and wireless mesh networks (WMNs). Since the network is infrastuctureless the routing becomes a major issue and these types of networks are very prone to several kinds of attacks. Hence the selection of appropriate routing protocol and encryption scheme is a major task. This paper presents a comparative performance analysis of Proactive, Reactive, and Hybrid protocols based on performance metrics like communication overhead, end to end delay (RTT) and throughput on various hybrid cryptographic combinations namely (AES-RSA),(AES-ECC) and (RSA-ECC).**

***Index Terms*: Routing Protocols, ANET, Cryptography, AES, RSA, ECC, SHA 256 etc.**

I. Introduction

A wireless network is one which establishes communication among the nodes wirelessly. These types of networks do not have a well defined infrastructural support to communicate among the nodes. To enable successful communication between the sender and receiver the route selection, route establishment decisions are done by negotiating all the other nodes in the network. Hence, nodes in wireless network need to be more intelligent so that they can act as a node to transmit, receive the data by routing packets to the other nodes, which makes them more complex as compared to cellular networks.

Providing security to these networks becomes a tedious task because they become vulnerable to attacks due to packet dropping, impersonation which degrades the network performance. This paper mainly focuses on the security analysis of hybrid cryptographic techniques on three widely used routing protocols namely AODV, DSDV and ZRP. Performance comparisons of the routing protocols are carried out based on the computational parameters like Round trip time, communication overhead and throughput.

II. Routing in ANETs

Routing is the phenomena of decision making to direct network packets from source to the destination. Routing is essentially classified as static and dynamic routing. Static routing is usually employed in smaller networks. In this, the routing tables are configured manually and routing of packets is done referring these routing tables. Public switch telephone network is one example that makes use of static routing.

On the contrary, in Dynamic Routing, the routing tables are constructed automatically using routing protocols such as Open Source Shortest Path First (OSPF), Routing Information Protocol (RIP), etc. The various type of routing protocols along with its classification is as shown in Figure 1. The responsibility of routing process or routing protocols is to exchange information, find an optimum path, repair broken paths, utilize minimum bandwidth, etc. There are few challenges also faced by theses routing protocols like bandwidth constraints, mobility, error prone and shared channel, computational power, battery power, scalability, security, privacy etc.

III. Routing Protocols

A. *Ad Hoc on Demand Distance Vector Routing Protocol (AODV)*

ANETS mainly make use of the AODV which supports both unicast and multicast routing. The route establishment is done On-demand that is only when source node requests for it. Routes are maintained until the source node requires them. Hence they do not create much traffic. All the nodes are silent until any connection gets established. Node that wants to communicate will request for connection. Remaining node will record the message and forwards it to other nodes, thus a temporary route gets created. A node that monitors the request will send a retrogressive message to the requested node. The requested node will utilize the route that has least number of hops to the destination node.

B. *Destination Sequenced Distance Vector (DSDV)*

It is an enhanced version of the distributed Bellman -Ford algorithm where each node maintains a table that contains the shortest distance and the first node on the shortest path to every other node in the network. It maintains table updates with increasing sequence number id's to prevent loops, oppose the count-to-infinity problem, and for faster convergence. As it is a table-driven routing protocol, routes to all destinations are readily available at every node at all times. The tables share their information between neighbours at regular intervals to keep an up -to-date view of the network topology. Table updates are initiated by a destination with a new sequence number which is always greater than the previous one.

C. *Zone Routing Protocol (ZRP):*

ZRP is a hybrid protocol that makes use of both proactive and reactive protocol. Here the nodes are divided into zones. If both the sender and receiver are in the same zone a proactive protocol is used to route the packets to the destination. A reactive protocol is used when both sender and receiver are in different zones. This protocol checks for each successive zone whether the node is present or no. Once the zone is confirmed that the node is present in it, the proactive protocol is used to route the packets. Hence it reduces the control overhead for longer routes [13].

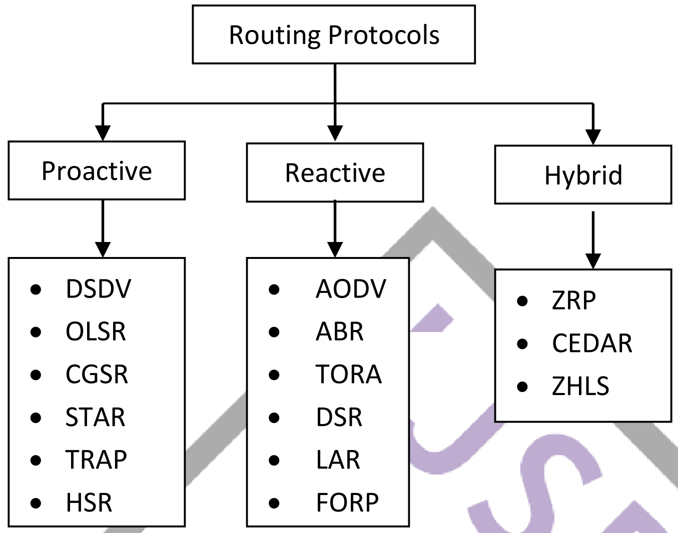

Figure 1: Types of Routing Protocols [7]

IV. LITERATURE SURVEY

In the paper titled, "A Dynamic Anomaly Detection Scheme for AODV-Based Mobile Ad Hoc Networks" authored by Hidehisa Nakayama, A new anomaly detection scheme depending on dynamic learning process that incorporates training data to be refreshed at specific time intervals is described. This involves the projection distances in view of multidimensional statistics using weighted coefficients and a forgetting curve. MANET simulations are conducted using Network Simulator and scenarios are considered for discovering five types of attacks. The effectiveness of the system is showed as the result [9].

In the paper titled, "Secure Data Transmission on MANET by Hybrid Cryptography Technique" authored by Ashish Sharma, Dinesh Bhuriya, Upendra Singh, a secure data transmission using hybrid cryptographic technique is proposed. AODV and SAODV protocol is used to maintain the routes in the nodes. The DES and RSA algorithms are used for encrypting the data to be transmitted. The parameters for both the AODV and SAODV are compared to give better performance for SAODV as compared to regular Ad Hoc On demand Distance Vector routing [5].

In the paper titled, "Cryptography Based Secured Advanced on Demand Routing Protocol in MANET's" authored by Prachi D. Gawande and YogeshSuryavanshi, a cryptographic system for MANETs using on demand routing protocol is proposed. Two routing protocols AODV and DSDV are used for routing in the network. AODV has certain characteristics which overcome the disadvantages of DSDV. Hence proves AODV to be a better performing protocol than compared to DSDV.RC6 technique is used to secure the network [6].

In the paper titled "An Intrusion Detection System for Wireless Sensor Networks" authored by IlkerOnat and Ali Miri, a detection based security plot for wireless sensor network is proposed. Since sensor nodes have low communication capability and due to specific properties like maintenance of neighbourhood information which makes anomaly detection easier. Such characters enable to provide security to large scale networks easily. Initially an attacker proves himself to be a legitimate node. Hence any sensor node should be capable of detecting an Intruder wherein a simple dynamic statistical model is built and also a low complex algorithm is used to monitor the power levels and the arrival rates of the received packets [10].

In the paper titled, "A Study of Intrusion Detection Systems in MANETs" authored by Umesh Prasad Rout, details that the use of MANETs has been continuously increasing, hence prevention systems are not enough defending system before there is any security breach, detection of these Intrusions is a must. This Paper makes a study on different Intrusion Detection Systems. Stand alone Intrusion detection runs on each node independently to find any malicious node present. In distributed and co-operative systems an agent detects and collects local events to identify Intrusions and initiate a response immediately and the other agentswill cooperatively participate in Global Intrusion detection systems. The Hierarchical Intrusion Detection systems is an extended version of Distributed and cooperative system which is mainly used for multi-layered networks and the whole network id divided in to clusters [11].

V. SECURITY SERVICES AND MECHANISMS EMPLOYED

Cryptography is a process of converting plaintext to cipher text and vice versa. Figure 2 shows different types of cryptographic techniques.

A. *Symmetric Cryptography:*

It involves algorithms that use the same key or functions for encrypting the message and decrypting the cipher text. Examples of algorithms using same keys or functions on sender and receiver end include Caesar cipher, DES(Data Encryption Standard), AES(Advanced Encryption Standard) etc.

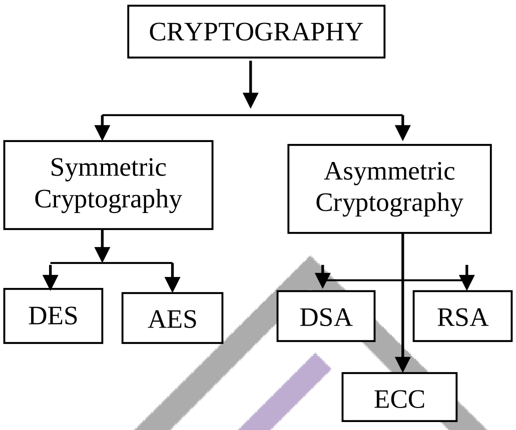

Figure 2: Types of Cryptography

a. AES(Advanced Encryption Standard)

AES was developed in the year 1999. It is a block cipher algorithm with block length of 128 bits and key lengths of 128,192 or 256 bits. The key length depends upon the number of rounds in algorithm.

In AES, each round contains four operations:

- **Sub Bytes-** this is a non-linear substitution, wherein each byte is replaced by another fixed bytes.
- **Shift rows-** In this, each row is rotated according to row position from left to right.
- **Mix Columns-** performs mixing operations on columns with constants and data.
- **Add Round key-**combining data's bytes column with a key's byte column[15].

B. *Asymmetric Cryptography:*

In asymmetric/public key Cryptography, two different keys are used. One is called a private key which is known by a single party and another is called as a public key which available to both the parties involved in communication. The public keys are shared among the parties by means of key management mechanism such as Diffie Hellman Key distribution.

Asymmetric cryptography includes DSA, RSA and ECC [7]. ECC is preferred more compared to RSA and/or DSA because of its smaller key size and faster computation speed with higher security. The following Table.1 depicts the comparative study of ECC, RSA/DSA and symmetric cryptography based on their key sizes.

Table 1: Comparable key sizes of Symmetric, ECC and RSA/DSA [7]

Symmetric (Key size in bits)	ECC (size of n in bits)	RSA/DSA (modulus size in bits)
56	112	512
80	160	1024
112	224	2048
128	256	3072
192	384	7680

a. RSA (Rivest, Shamir, Adelman)

RSA is a popular Asymmetric encryption method that uses very large prime numbers to generate public and private keys. This algorithm was programmed by Ronald Rivest, Adi Shamir and Leonard Adelman. This algorithm based on concept of factoring, making it easy to encrypt but hard to be decrypt. RSA is one of the hardest algorithm that robust, and difficult to crack of the encryption standards currently used by application for secure storage and transmission of data.

b. Elliptic Curve Cryptography (ECC)

Elliptic curve cryptography (ECC) is asymmetric key cryptography by nature and is considered as a marvellous technique with low key size for the user, and has a hard exponential time challenge for an intruder to break into the system.

It was proposed by Miller and Koblitz. Elliptic curve cryptography is not easy to understand by attacker, so it is not easy to break. In ECC a 224-bit key provides the same security as compared to the traditional crypto system RSA with a 2048-bit key, thus lowers the computer power[4]. Therefore, ECC offers considerably greater security for a given key size. Consequently, a key with smaller size increases the possibility of compact implementations for a given level of security, which means faster cryptographic operations, running on smaller chips or more compactsoftware. Further, they are considered to be extremely efficient.

C. Secure Hash Algorithm(SHA 256)

SHA-256 (secure hash algorithm) is a cryptographic hash function with digest length of 256 bits. In other words, these are termed as novel hash functions computed with 32-bit words. It is a keyless hash function; that is, an MDC (Manipulation Detection Code).

IV. PERFORMANCE ANALYSIS

In this section, the performance of various routing protocols with respect to certain network parameters for different combinations of hybrid cryptography is discussed.

1. ***Communication Overhead****:* The total number of packets that are to be transferred or transmitted from one node to another is known as the **communication overhead**. It includes the **overhead** of routing process, routing table and packet preparation in a sensor node. From Tables 2, 3 and 4, it can be seen that the *Communication Overhead* is highest in DSDV protocol for any combination of hybrid cryptography.

Table 2: Parameters Comparison of AODV, DSDV & ZRP: AES-ECC

AES-ECC	**AODV**	**DSDV**	**ZRP**
Communication Overhead	42	671	7
Round Trip Time (sec)	26	17	11
Throughput (%)	28	37	20

Table 3: Parameters Comparison of AODV, DSDV & ZRP: AES-RSA

AES - RSA	**AODV**	**DSDV**	**ZRP**
Communication Overhead	42	671	7
Round Trip Time (sec)	23	16	10
Throughput (%)	30	37	32

2. ***Round Trip Time****:* It is the total time taken by the message to reach the destination plus the time taken for the acknowledgement of the message to be received. From Tables 2, 3 and 4, it can be seen that the RTT is highest in AODV protocol for any combination of hybrid cryptography.

Table 4: Parameters Comparison of AODV, DSDV &ZRP: RSA-ECC

RSA - ECC	**AODV**	**DSDV**	**ZRP**
Communication Overhead	42	671	7
Round Trip Time (sec)	27	20	22
Throughput (%)	30	37	23

3. ***Throughput****:* It is the measure of total data received at the receiver to the total time taken. Tables 2, 3 and 4, it can be seen that the throughput is highest in DSDV protocol for any combination of hybrid cryptography.

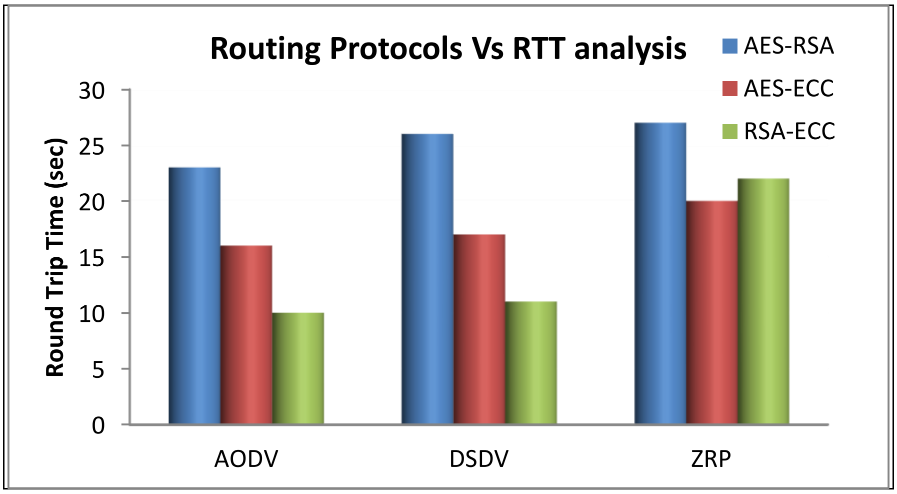

Figure 4: RTT Analysis of Routing Protocols with Hybrid Cryptography

4. ***Route Maintenance:*** It is the property of the network to form new links or connections in case of breakage of link or addition of a new node to enhance the strength of the existing network along with its capacity. Table 5 depicts the delay caused in the network due to addition of new node.

Table 5: Route Maintenance Delay Comparison of Routing Protocols

Route Maintenance Delay (secs)	AODV	DSDV	ZRP
AES - ECC	120	1810	9
AES - RSA	119	1805	8
RSA - ECC	199	1804	7

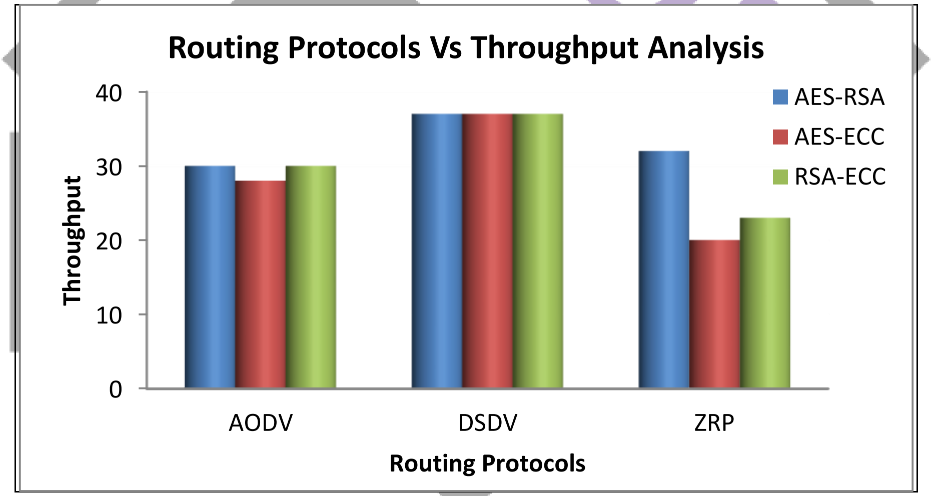

Figure 5: Throughput Analysis of Routing Protocols with Hybrid Cryptography

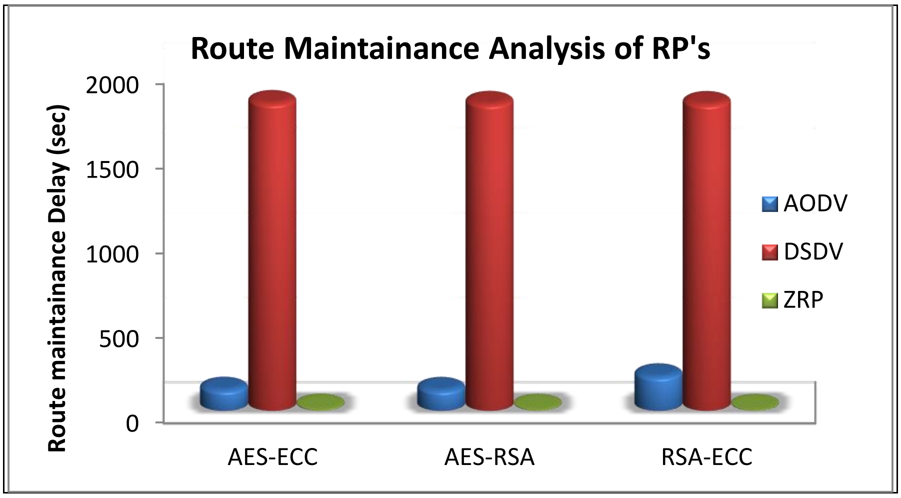

Figure 6: Route Maintenance Analysis of Routing Protocols with Hybrid Cryptography

Table 6 illustrates the overall comparison of various routing protocols with respect to the parameters mentioned above.

Table 6: Overall Comparison of AODV, DSDV & ZRP

Parameters	AODV	DSDV	ZRP
Protocol Type	On demand	Table driven	Hybrid
Network Type	None	None	Zone based
Data Encoding /Decoding	(AES-RSA) (AES-ECC) (RSA-ECC)	(AES-RSA) (AES-ECC) (RSA-ECC)	(AES-RSA) (AES-ECC) (RSA-ECC)
Hashing	SHA-256	SHA-256	SHA-256
Control Overhead	High	Very high	Less
Latency	High	Moderate	Less Compared to AODV
BW consumed	High	High	Less
Attack Detection	Takes more time	Early detection than ZRP	Early detection

CONCLUSION AND FUTURE SCOPE

We know that routing protocols play a very important role in communication over the network and cryptography helps in securing the communication over the network. There are a number of protocols available for data communication, and the selection of a suitable protocol for a given network application is an essential factor to enhance the performance of the network.

In this work, Hybrid Cryptographic Technique is implemented and the performance analysis is carried out for three combinations of the hybrid scheme namely; (AES-RSA), (AES-ECC) and (RSA- ECC) to enhance the security of data transmitted over the network. These combinations are tested on three routing protocols namely AODV, DSDV and ZRP. In addition, SHA-256 hash function is also deployed in order to maintain data integrity. It can be seen that the hybrid combination of algorithms along with hash function proves to be much more secure than the individual cryptography algorithms as this produces a fixed length cipher for any given length of message, thus; making it difficult for the attacker to guess the actual length of message.

Extensive simulation is carried out and the results are tabulated for various hybrid combinations for each protocol. The results convey that, for any hybrid combination, ZRP offers least communication overhead along with least delay (RTT) as compare to AODV and DSDV, because of its path optimization feature and hence it is more preferred in dense networks. However, DSDV is shown to offer highest throughput, in comparison with the other two protocols considered. The reason for this is, its proactive naturewhich enables the network to find the routing path easily with the use of routing tables formed.

Future work can be done on other combinations of cryptographic algorithms and test them on various performance metrics like encryption and decryption time, round trip time and throughput by considering other routing protocols.

REFERENCES

[1] Anup Ashok Patil, Shital Mali, “Hybrid Cryptography mechanisms for securing self organied wireless networks”, 3rd International Conference on Advanced Computing and Communication Systems (ICACCS), January 22 – 23, 2016.

[2] Elhadi M. Shakshuki, NanKang,andTarek R. Sheltami, “EAACK— A Secure Intrusion-Detection System for MANETs”, IEEE Transactions on industrial electronics, volume 60, issue 3, pp 1089-1098, March 2013.

[3] Adnan Nadeem and Michael P. Howarth, “A Survey of MANET Intrusion Detection and Prevention Approaches for Network Layer Attacks”, IEEE Communications Surveys and Tutorials, volume 15, issue 4, pp 2027-2045, 2013.

[4] MeghaKolhekar, Anita Jadhav, “Implementation of Elliptic Curve Cryptography on Text and Image”, International Journal of Enterprise Computing and Business Systems, volume 1, issue 2, pp 2230-8849, July 2011.

[5] Ashish Sharma, Dinesh Bhuriya, Upendra Singh, “Secure Data Transmission on MANET by Hybrid Cryptography Technique”, IEEE International Conference on Computer, Communication and Control (IC4) 2015.

[6] Prachi D. Gawande, YogeshSuryavanshi, “Cryptography Based Secured Advanced on Demand Routing Protocol in MANET's” IEEE ICCSP, pp 1478-1481, 2015.

[7] William Stallings, “Cryptography and Network Security”, Fourth Edition, June 3, 2010.

[8] Padma Bh, D.Chandravathi , P.PrapoornaRoja, **“**Encoding And Decoding of a Message in the Implementation of Elliptic Curve Cryptography using Koblitz’s Method”,(IJCSE) International Journal on Computer Science and Engineering, volume 2, issue 5, 2010.

[9] Hidehisa Nakayama, “A Dynamic Anomaly Detection Scheme for AODV-Based Mobile Ad Hoc Networks” IEEE Transactions on Vehicular Technology, volume 58, issue 5, pp 2471-2481, June 2009.

[10] IlkerOnat, Ali Miri “An Intrusion Detection System for Wireless Sensor Networks”, International Conference on Wireless and Mobile Computing, Networking and Communications, IEEE, August 2005.

[11] Umesh Prasad Rout, “A Study of Intrusion Detection Systems in MANETs”, International Journal of Research in Computer and Communication Technology, volume 2, Issue 2, pp 86-92, February 2013.

[12] ChristoforosPanos, Christos Xenakis, IoannisStavrakakis, “A Novel Intrusion Detection System For MANETS”, Proceedings of the International Conference on Security and Cryptography (SECRYPT), IEEE Athens, Greece, 2010.

[13] Murthy, C.S.R, “Ad-hoc Wireless Networks: Architectures and Protocols”, 2004.

[14] Rani, S. and Kaur, H., 2017. Implementation and comparison of hybrid encryption model for secure network using AES and Elgamal. International Journal, volume 8, issue 3, 2017.

[15] Bhole, D., Mote, A. and Patil, R., “A New Security Protocol Using Hybrid Cryptography Algorithms”.

[16] Kaur, S., Bharadwaj, P. and Mankotia, S, “Study of Multi-Level Cryptography Algorithm: Multi-Prime RSA and DES”, International Journal of Computer Network and Information Security, volume 9, Issue 9, p.22, 2017.

[17] Jain, M and Agrawal, A,Implementation of hybrid cryptography algorithm. International Journal of Core Engineering & Management (IJCEM), volume 1, issue 3, pp.126-142, 2014.

[18] Zuhi Subedar, Satish Deshpande, “Hybrid Cryptography Approach for securing MANETs-A Survey” IJIRCCE, Volume 6, Issue , January 2018.