Secure and Energy Efficient Communication in Wireless Sensor Network

Mukesh Patil
Dept. of Computer Engg. Student
Smt. KashibaiNavale College of Engineering, Pune-411041

Nalini A. Mhetre
Professor
Assistant Professor
Smt. KashibaiNavale College of Engineering, Pune-411041

ABSTRACT
Cryptographic data transmission from one node to another node in a secure way is the challenging goal in Wireless Sensor Network (WSN). In WSN security is achieved through Message Authentication Code (MAC) as well as Encryption algorithm. Consolidation of MAC and Encryption strategy will provide the high security for data or message which is used for communication. In communication system, confidentiality of data and cost of transmission of data are the key aspects. Along with the security, energy is also the major challenge in WSN. In WSN sensor nodes have the small amount of resources such as bandwidth, power etc. Hence conservation of energy and establishment of security are two major parameters in WSN. This paper proposes the details of the shortest path generation algorithm, which efficiently satisfies mentioned constraints and security is established using ECC algorithm.

General Terms
WSN, efficiency, security.

Keywords
Security, message authentication code (MAC), WSN, universal hash function, authenticated encryption, Elliptic curve cryptography.

1. INTRODUCTION
In cryptography, the important objective is to provide the privacy to messages transferred in public networks. To maintaining the privacy, Message Authentication Code (MAC) is the main concept for data security. MAC has the main features to maintaining the integrity and confidentiality of the message. It is necessary to provide security to MAC which protects the messages against controverted with high computational power.

Dedicated approach and generic approach are the two main approaches for building new secure transmission channel in cryptography. The generic approach can be built in three different way such as Encrypt and authenticate (E&A), Encrypt then authenticate (EtA), or Authenticate then Encrypt (AtE). The advantages of generic approach over dedicated approach are the faster implementation of authenticated encryption when fast encryption algorithm use [1]. Secure MACs calculation methods, keys can be used for verification of self-assertive messages. That means, in the wake of conceding to key, valid users can interchange a number of confirmed messages with the same key. This is efficiently applicable on sensor network for the real-time application.

Based on numbers of distributed independent sensor nodes, the remote sensor network is built. Sensor nodes have the ability to sense the data, process it and then communicate with another node. These sensor nodes keep the track record of physical as well as environmental activities combine and continuously. Activities may have sound, temperature, motion and so on. WSN is the backbone of emerging technologies like Internet of Things (IoT), Cyber physical system (CPS) etc.

In WSN routing is a difficult task. Designing a routing protocol for WSN is different from designing it for the traditional networks. Therefore, resource management is very important for designing a routing protocol for WSN. The main motive behind the routing is a route selection and data forwarding. Select the best route between two nodes are the main function of route selection method. A sensor node reads data and sends it to the next node or hop by making use of multi-hop routing. The main purpose of using sensor nodes is to monitoring. Sensor applications such as weather, wild animal's surveillance monitoring system and so on make use of sensor nodes to get real-time activities. So it is important for the sensor nodes to have different attributes such as energy, memory, computational power etc. Sensor node sense the data then process it and then pass to the neighbor node and so on. To transmit the data from one node to another node in a secure manner is the main goal of this paper. Because of its limited power, we find out the efficient way to transmit data and save the energy of sensor node.

In this paper, section II describes Motivation. The related work done in literature is explaining the section III. In section IV describes the problem statement. Section V describes the proposed work with system architecture, algorithm. Mathematical Model describe in Section VI. Section VII shows the results of our system. Finally section VIII concludes our system.

2. MOTIVATION
Lately communication in multiple humans happens by using postcard conversation but the downside with this system was forgery of the message, it means data was not secure. Hence there is scope in establishing or developing secure in communication mechanism in current communication system such as email, sensor communication etc. The users who are registered and valid in behavior can only able to take part in the communication.

3. RELATED WORK
Verification of numerous messages m1, m2, … , m_L where every message m_i is a set of bit s [2]. Author outlined a plan for the creation of a message authentication code (MAC) tag t, of m1, m2, … ,m_L. It takes consistent (autonomous of L) and has a tag length. The tag length of message is consistent or not dependent of the L. The check time of the plan generation is additionally constant. The plan uses an updated version of division by an irreducible polynomial over GF(2) considering the end goal to pack the messages. The packed outcome

becomes data to a pseudo random function Fk(.) to get a safe tag t. System proves that the security of the proposed MAC plan is to achieve. The plan having the different applications in sensor systems where distinct messages give with the single tag. Various numbers of bits transmitted by a sensor node, consequently diminishing force uses at the sensor node. Another application is multimedia authentication system. In this application, multimedia information is divided into small parts and each part is allocated with individual MAC.

Channel with high security increase the confidentiality and authenticating message share from valid user discussed in [3]. A bland methodology of combining so as to build such channels. It is an encryption primitive with an authentication primitive (MAC). This system gives the configuration of cryptographic primitive utilized for the development of secure channels. Instead, broad useful MACs use the extra ordinary MACs known as ϵ-MACs. As the message should be encoded and validated, there should repetition while computing by two attributes. Along these lines, uprooting such excess can maximize the proficiency of the commonly speaking synthesis. In addition, computation carried out by the encryption computations can be utilized to maximize the security of the confirmation computation. Specifically, Author will indicate how ϵ-MACs can be intended to lessen the measure of computation needed by standard MACs taking into account general hash capacities.

Jun Deng, Rongqing Zhang proposed [4], to makes sure of security while sending data. This is the most important problem for wireless networks. Physical layer security is famous options answer for location this problem. In this paper, they assume a helpful method, comprising a source node, a destination node, one eavesdropper node, also different relay nodes. In particular, the source may select fewer transfers to forward the sign to the comparing destination to accomplish the best security execution. Although, the transfers might have the motivation not to report their actual private direct data taking in account end goal to get more chances to be selected and acquire outcome from the source. The author proposes a component depending on Vickey-Clark-Grove (VCG) as well as an Arrow-d'Aspremont- Gerard-Varet (AGV) based component in the relay network. These two attributes are utilized to overcome the security problem. In these instruments, they plan diverse "transfer payment" capacities to the result of each chose transfer and shows that every hand-off gets its most extreme payoff when it honestly uncovers private channel data to the source. After that, ideal mystery rate of the framework can be completed. In the wake of talking about and contrasting the VCG and AGV technique, they showed that AGV component can accomplish the large part of the basic capabilities for a system. Basic capabilities have impulsive compatibility, rationality and budget balance. Along with, Author examines the ideal amount of send that the source hub should select. Recreation results provide productivity and decency of the VCG and AGV components and solidify these conclusions.

Author [5], implants a method for encrypted short messages authentication. This method is applicable to numerous mobiles as well as pervasive applications. For the authentication messages should be in encrypted format. Secure authentication code created by developed system is more efficient than the code created by existing systems in literature. To get this, system adding short string randomly after plaintext message before encrypting it. It gives results in more efficient authentication.

The trust management systems for WSNs discussed in [6]. This system provides security against attacks. It efficiently manages the resources including processing power and storage. The trust is used as a tool. Trust provides better security by supporting to routing protocols. Recently many researchers point of interest is to find out more reliable solutions related to trust. In addition, they enhanced the techniques which are implementing the trust frameworks. Moreover, they provide designed trust systems with comparisons and summary.

Implements an idea which utilizes session keys taken from expert keys to set up a group key that is data hypothetically secure [7]. At the point when expert keys are dispersed, system needs O(logb t) multicasts, where $(1 - 1/b)$ is probability that a given customer has a given master key. The base number of open multicast transmissions is required for an arrangement of clients.

Stretches out stage encryptions to general remote correspondence methods does not depend on modulation method which built in [8]. They get the term XOR-Enc and P-Enc for effortlessness to show XOR and phase encryption, differently. They appear P-Enc used under their setting can be reached out to amplitude shift keying (ASK), phase shift keying (PSK) and quadrature amplitude regulation adjustments, yet not to frequency shift keying (FSK) balance.

Author of [8] implements authentication scheme for time basic verification of command and control messages. System work quick verification. System finds out the semi structured command and control messages. This is utilized to generate the uncommon digital signature. It is computationally effective at signer and verifier sides. They show that Random Authentication (RA) has a few advantages attributes which are not accessible in existing choices all the while: quick signature generation and confirmation; quick check; consistent size public key; conservative validating tag; packet loss tolerance; being free from time synchronization necessity and provable security.

In [9] system examines key and forgery attacks recovery on the some MAC computations. It is depending on universal hash functions. The attacks uses a considerable verification questions yet in the long run take into account universal forgeries instated of different forgeries. This represent the security of computation totally collapses once a couple of forgeries are found.

Table1 Evaluation Table

Reff. Num.	**Parameter**			
	Time Complexity	**Energy Efficiency**	**Key Length**	**Techniques**
[1]	Constant	No	N bit	Generate the tag for multiple message.
[2]	-	No	-	ϵ- MAC for generating tag
[4]	O(log n log log n)	No	-	Encryption by CBC.
[7]	$O(\log_b t)$	Low	Not	Established

			Fixed	group key among 't' client.
[9]	-	Low	-	Universal hash function
Proposed work	$O(n^2)$	High	Variable	E&A, EtA, AtE by ECC

4. PROBLEM STATEMENT

Presently, many applications rely on the existence of small devices that can exchange information and form communication network. It is very challenging to provide security for such application. IN significant portion of such applications, the confidentiality and integrity of the communicated messages are of particular interest. In this proposed system which increased the security of the application. Here proposed algorithm which increases the security performance of MAC algorithm. We also reduced the energy consumption by network.

5. PROPOSED WORK

5.1 System Overview

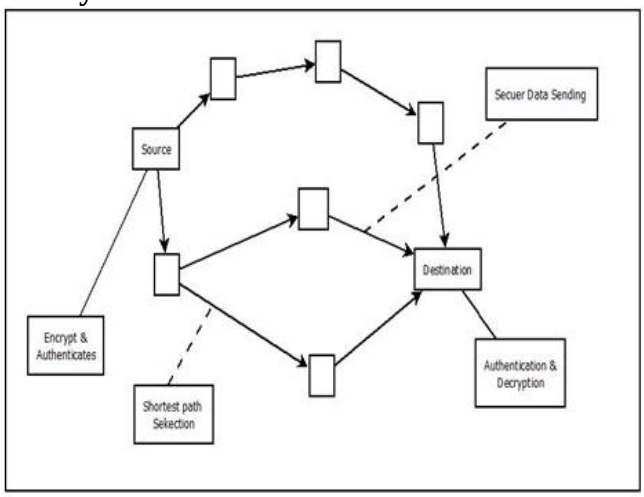

Fig.1 System Architecture

Fig. 1 shows the system architecture of proposed system. Detail description of system as follows:

- Network Creation: In network creation vertices or nodes are linked with the edges.
- All path generation: After creating the source and destination, create all possible path from source to destination.
- Get shortest path: Search shortest path from source to destination from all generated paths.
- Key generation and distribution: Key generation center generates the key and distributes the key to source node. Perform the route generations from source to the destination.
- Message encryption: Message is generated at source node. After generating the message, message encrypted at source node by using the ECC algorithm.
- Hash value generation: Generate the hash value of message and send it to destination.
- Energy consumption: Calculate total energy consumption by each sensor node in shortest path.
- Message decryption: At destination, decryption of message with appropriate key.

5.2 Algorithm

5.2.1 Proposed algorithm

- Generate the network. Network represented as graph which includes number of vertices connecting with edge.
- Selection of Source and Destination from all nodes.
- Generate all possible paths from source node to destination.
- Select feasible shortest path among all generated paths.
- Generate pair of public and private keys and assign to source and destination.
- Create the message at source. Encrypt the message and generate hash value of message.
- Send key and hash value to destination via shortest path.
- Calculate energy consumed by each node present in shortest path.
- First way, authenticate hash value of received message and encrypted message at destination node and decrypt the message.
- Second way, generate hash value of encrypted data and authenticate hash value of received message at destination node.
- Third way, generate hash value of message and encrypt that hash value and authenticate cipher text of hash value.
- Calculate energy consumption and time complexity at each node.

Above algorithm describes the steps of the proposed system. Initially network is generated with sensor nodes. Then source and destination nodes are identified along with generation of all paths from source to destination and select the shortest path for message sending purpose. Calculate consumed energy. System encrypts the message by using the ECC algorithm. Message forwards from source to destination by using three different ways. First way, generate hash value of message and encrypted message send to destination node and authenticate both encrypted message and hash value at destination node. Second way, generate hash value of encrypted message and authenticate hash value of received message at destination node. Third way, generate hash value of message and encrypt that hash value and authenticate cipher text of hash value. If the message is not verified that message is rejected.

5.2.2 Elliptic curve cryptography (ECC) algorithm

- Sender and Receiver Computed S = (S1, S2).
- Sender sends a message M to Receiver as follows:

  Compute (S1 * S2) mod N = K

  Compute K * M = C, and send C to Sender
- Receiver receives C and decrypts it as follows:

  Compute (S1 * S2) mod N = K.
  Compute (K-1)mod N
  (Where N = E)
- K-1*C = K-1*K*M = M.

6. MATHEMATICAL MODEL

System S is a set of {N, S, D, P, Sp, K, d}

- Deploy nodes

  N = {n1, n2, ... ,nn }

  N = set of all deployed nodes.
- Source node creation

  S = {s1, s2, …….,sn}

  S = a set of all Sources.
- Destination node creation

  D = {d1, d2, ...,dn}

  D = a set of all sink node
- Find all Possible Paths

  P = {p1, p2,....,pn}

  P = a set of all Paths
- Selection of Shortest Path

  Sp = {sp1, sp2, sp3, ...,spn}

  Sp= set of all Shortest Path
- Identify set of MAC generated

  MAC ={ mac1,mac2,.....,macn}

  Where MAC is set of all hash values(MACs)
- Identify the set of Encrypted Key

  E= {e1, e2, e3….}

  E represents the main set of Encrypted Key.
- Identify set of decryption key

  DK= {dk1, dk2, dk3….}

  DK represent the main set of Decryption key.
- Calculate residual energy of each node

The energy spent of a node that transmits l-bits packet over distance d is:

$$E_{Tx}(l,d) = E_{Tx-elec}(l) + E_{Tx-amp}(l,d)$$
$$= E_{elec} * l + \in_{fs} d(2) * l$$

- Where, with amplifying index $\in_{fs}$, $\in_{mp}$ respectively

$$d_0 = \sqrt{\frac{\in_{fs}}{\in_{mp}}}$$

- And the energy consumption of receiving this message is:

$$E_{Rx}(l) = E_{elex} *$$

- Distance formula:

$$D = \sqrt{(x_2 - x_1)^2 + (y_2 - y_1)^2}$$

Note: Here the node which has maximum energy from the network is selected as a gateway.

7. RESULTS

7.1 Energy consumption graph

Fig. 2 shows the comparison graph for energy consumption ratio of existing and proposed system. In the existing system energy consumption ratio is more as compare to the energy consumption ratio in the proposed system.

Table2 Energy Consumption Table

Parameters	Existing	Proposed
Energy Consumption	435	245

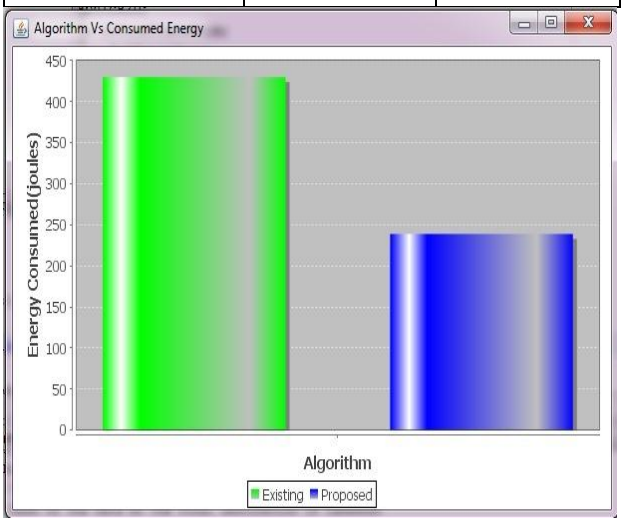

Fig.2 Energy consumption graph comparison

7.2 Time graph

Fig. 3 shows the comparison graph for Time graph of existing and proposed system. In the existing system Time ratio is more as compare to the Time in the proposed system.

Table3 Time Evaluation Table

Parameters	Existing	Proposed
Total time	220	170

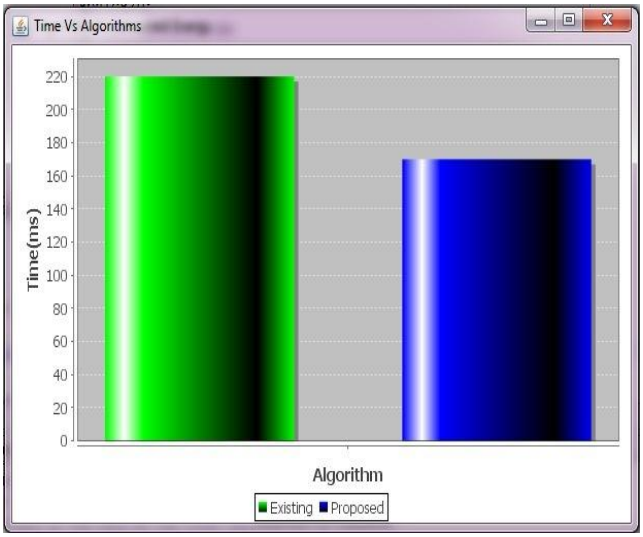

Fig.3 Time graph comparison

8. CONCLUSION

Present system gives security by utilizing common conventions, but this system has its own sit downs like large energy utilization in pervasive environment. So we proposed shortest path calculation in network system which minimized energy utilization of nodes. We also maximized the security at the time of data sending from source to destination through MAC and Encryption algorithm. Secure communication gives in pervasive application by using ECC algorithm. In future, we can improve more network lifetime and secure communication.

9. ACKNOWLEDGMENTS

I would like to thank the researchers as well as publishers for making their resources available and teachers for their valuable guidance. We also thank the college authorities for providing the required infrastructure and support. Finally, we would like to extend a heartfelt gratitude to friends and family members.

10. REFERENCES

[1] H. Krawczyk, "The Order of Encryption and Authentication forProtecting Communications (or: How Secure Is SSL?)," Proc. 21stAnn. Int'l Cryptology Conf. (CRYPTO '01), pp. 310-331, 2001.

[2] Aida Vosoughi, RajendraKatti,"Fast Message Authentication Code for Multiple Messages with Provable Security", IEEE Globecom 2010 proceedings J. Clerk Maxwell, A Treatise on Electricity and Magnetism, 3rd ed., vol. 2. Oxford: Clarendon, 1892, pp.68-73.

[3] RadhaPoovendran Senior Member, IEEE and Basel Alomair, Member, IEEE," ϵ-MACs: Toward More Secure and More Efficient Constructions of Secure Channels", 204 IEEE transactions on computers, Vol. 63, No. 1, JANUARY 2014.

[4] Jun Deng, Rongqing Zhang, (*Student Member, IEEE)*, Lingyang Song, (*Senior Member, IEEE)*, Zhu Han, (*Senior Member, IEEE)*, and Bingli Jiao, (*Senior Member, IEEE),"* Truthful Mechanisms for Secure Communication in Wireless Cooperative System", IEEE transactions onwirelesscommunications, Vol. 12, No. 9, September 2013.

[5] B. Alomair and R. Poovendran, "Efficient Authentication for Mobile and Pervasive Computing," Proc. 12th Int'l Conf. Information and Comm. Security (ICICS '10), 2010.

[6] P. Raghu Vamsi and Krishna Kant "Systematic Design of Trust Management Systems for Wireless Sensor Networks: A Review", Fourth International Conference on Advanced Computing Communication Technologies, 2014.

[7] Attila Altay Yavuz, ``An Efficient Real-Time Broadcast Authentication Scheme for Command and Control Messages", IEEE transactions on information forensics and security, vol. 9, No. 10, October 2014.

[8] Thomas R. Halford, Thomas A. Courtade, Keith M. Chugg, Xiaochen Li, and GautamThatte, ``Energy-Efficient Group Key Agreement for Wireless Networks", IEEE transactions on wireless communications, vol. 14, NO. 10, October 2015.

[9] FeiHuo and Guang Gong, ``XOR Encryption Versus Phase Encryption, an In-Depth Analysis" IEEE transactions on electromagnetic compatibility.

[10] Helena Handschuh and Bart Preneel, ``Key-Recovery Attacks on Universal Hash Function Based MAC Algorithms", International Association for Cryptologic Research 2008.

[11] Bowman, M., Debray, S. K., and Peterson, L. L. 1993. Reasoning about naming systems.