# An Improved Novel Design for user Authentication and Secure Transmission of Data in End to End Routing in Wireless Sensor Network

K RupaRani[1], K. Jagdeeshwara Rao [2]

*Final M.Sc. Student[1], Lecturer [2]*

*[1, 2] M. Sc Computer Science, Chaitanya Women's PG College, Old Gajuwaka, Visakhapatnam Andhra Pradesh*

***Abstract:***

*Now a day's wireless sensor network is most important technology for transferring data through network with secure manner. Before transferring message from source node to destination node we can find out path consisting of connected links. To identify the routing from source node to destination node so many end to end routing protocols are existing in the world. In this paper we are implementing a novel design secure end to end routing protocol for transfer data with securely. Before performing data transformation process we can implement two more fundamental concepts are user authentication and key establishment. The user authentication process enables for identify users by group key manager. After completion of authentication process the group key manager will generate polynomial equation for establishing secret session key and shared that key to all communication entities. Such that all communication entities will exchange information can be protected using this secret key. Before transferring data to destination node the source will send ids to group key manager. The group key manager will find routing from source node to destination node, using that path data will be transferred to destination node. Before transferring message the source node will encrypt the message and send to destination node. By performing data encryption and decryption process we are using cryptography technique. So that by implementing those concepts we can improve efficiency of network and also provide more security of transferred message.*

**Keywords:** *Group Key Generation, Secrecy of Data, End to End Routing, Source Node, Destination Node.*

## I. INTRODUCTION

Wireless sensor network (WSN) is widely considered as one of the most important technologies for the twenty-first century . In the past decades, it has received tremendous attention from both academia and industry all over the world. A WSN typically consists of a large number of low-cost, low-power, and multifunctional wireless sensor nodes, with sensing, wireless communications and computation capabilities. These sensor nodes communicate over short distance via a wireless medium and collaborate to accomplish a common task, for example, environment monitoring, military surveillance, and industrial process control. The basic philosophy behind WSNs is that, while the capability of each individual sensor node is limited, the aggregate power of the entire network is sufficient for the required mission. In many WSN applications, the deployment of sensor nodes is performed in an ad hoc fashion without careful planning and engineering. Once deployed, the sensor nodes must be able to autonomously organize themselves into a wireless communication network. Sensor nodes are battery-powered and are expected to operate without attendance for a relatively long period of time. In most cases it is very difficult and even impossible to change or recharge batteries for the sensor nodes. WSNs are characterized with denser levels of sensor node deployment, higher unreliability of sensor nodes, and sever power, computation, and memory constraints. Thus, the unique characteristics and constraints present many new challenges for the development and application of WSNs.

Due to the severe energy constraints of large number of densely deployed sensor nodes, it requires a suite of network protocols to implement various network control and management functions such as synchronization, node localization, and network security. The traditional routing protocols have several shortcomings when applied to WSNs, which are mainly due to the energy-constrained nature of such networks . For example, flooding is a technique in which a given node broadcasts data and control packets that it has received to the rest of the nodes in the network. This process repeats until the destination node is reached. Note that this technique does not take into account the energy constraint imposed by WSNs. As a result, when used for data routing in WSNs, it leads to the problems such as implosion and

overlap . Given that flooding is a blind technique, duplicated packets may keep circulate in the network, and hence sensors will receive those duplicated packets, causing an implosion problem. Also, when two sensors sense the same region and broadcast their sensed data at the same time, their neighbours will receive duplicated packets. To overcome the shortcomings of flooding, another technique known as gossiping can be applied . In gossiping, upon receiving a packet, a sensor would select randomly one of its neighbours and send the packet to it. The same process repeats until all sensors receive this packet. Using gossiping, a given sensor would receive only one copy of a packet being sent. While gossiping tackles the implosion problem, there is a significant delay for a packet to reach all sensors in a network. Furthermore, these inconveniences are highlighted when the number of nodes in the network increases.

Our focus is on routing security in wireless sensor networks. Current proposals for routing protocols in sensor networks optimize for the limited capabilities of the nodes and the application specific nature of the networks, but do not consider security. Although these protocols have not been designed with security as a goal, we feel it is important to analyse their security properties. When the defender has the liabilities of insecure wireless communication, limited node capabilities, and possible insider threats, and the adversaries can use powerful laptops with high energy and long range communication to attack the network, designing a secure routing protocol is non-trivial. We present crippling attacks against all the major routing protocols for sensor networks. Because these protocols have not been designed with security as a goal, it is unsurprising they are all insecure. However, this is non-trivial to fix: it is unlikely a sensor network routing protocol can be made secure by incorporating security mechanisms after design has completed. Our assertion is that sensor network routing protocols must be designed with security in mind, and this is the only effective solution for secure routing in sensor networks

## II. RELATED WORK

Currently, the progression of wireless technology in various application areas including military, industrial, environmental, medical, crisis management, smart environments to name but a few, leads to the emergence of wireless sensor networks (WSNs) at an accelerated pace to collect and communicate information from remote locations wirelessly. A wireless sensor network (WSN) can be treated as a co-operative network of small size, low power, smart devices named as Nodes or Motes, which have the capability of sensing a physical phenomenon (like temperature, humidity, pressure, vibration…etc) and relay the same or processed information to a sink via wireless links possibly with multiple hops between these nodes. The unique characteristics of WSN such as small size, low power consumption, autonomous, mobility, dense in volume, self-healing and self-organizing poses some constraints in terms of power consumption, storage, processing capabilities and bandwidth requirement. Even though energy efficiency is of a major concern, providing the required Quality of Service (QoS) in terms of timeliness, reliability, fault tolerance, is also of a major concern for the respective applications. For an instance, a wireless sensor network which is deployed in a nuclear power plant to monitor the release of radioactive fluids, has to detect the leakage at an infant stage and the corresponding alert has to relay to the control room with in a defined dead time, otherwise it may cause catastrophic effect. Likewise, WSNs have gained an immense attention for their ability in meeting the real time QoS guarantee in many time critical scenarios. In general, real time packet communication guarantee can be categorized as i) Hard Real Time (HRT) ii) Soft Real Time (SRT) . HRT should support a deterministic dead time. That implies, delivery of a message after the dead time is considered as a failure, sometime it may lead to a catastrophic effect. On the other hand, SRT supports probabilistic dead time, which allows some sort of latency in message delivery. Providing a real time communication in case of WSNs is a challenging task because of the highly unpredictable nature of wireless links, variable data packets relaying and energy, bandwidth constraints . The requirement of real time guarantee can be addressed from different mechanisms in different layers of protocol stack of WSN. I.e. by means of an efficient protocol in MAC layer, efficient routing protocol in network layer, by in network data aggregation mechanism and even cross layer design approach . In this paper, we presented a comprehensive survey of various real time routing protocols in WSNs, which meets the requirement of timeliness along with other QoS in time critical applications.

Routing is another very challenging design issue for WSNs. A properly designed routing protocol should not only ensure a high message delivery ratio and low energy consumption for message delivery, but also balance the entire sensor network energy consumption, and thereby extend the sensor network lifetime Motivated by the fact that WSNs routing is often geography based, we propose a geography-based secure and efficient Cost-Aware SEcure routing (CASER) protocol for WSNs without relying on flooding. CASER allows messages to be transmitted using two routing strategies, random walking and deterministic routing, in the same framework. The distribution of these two strategies is determined by the specific security requirements. This scenario is analogous to delivering US Mail

through USPS: express mails cost more than regular mails; however, mails can be delivered faster. The protocol also provides a secure message delivery option to maximize the message delivery ratio under adversarial attacks. In addition, we also give quantitative secure analysis on the proposed routing protocol based on the criteria proposed in Routing is a challenging task in WSNs due to the limited resources. Geographic routing has been widely viewed as one of the most promising approaches for WSNs. Geographic routing protocols utilize the geographic location information to route data packets hop-by-hop from the source to the destination. While geographic routing algorithms have the advantages that each node only needs to maintain its neighbouring information, and provide a higher efficiency and a better scalability for large scale WSNs, these algorithms may reach their local minimum, which can result in dead end or loops. To solve the local minimum problem, some variations of these basic routing algorithms were proposed in. In , source-location privacy is provided through broadcasting that mixes valid messages with dummy messages. The main idea is that each node needs to transmit messages consistently. Whenever there is no valid message to transmit, the node transmits dummy messages. The transmission of dummy messages not only consumes significant amount of sensor energy, but also increases the network collisions and decreases the packet delivery ratio. The (SEEM)] routing protocol has three types of nodes such as sensor node, sink node and base station node. The base station plays an important role in finding multiple paths between the source and the sink node. The control overhead is very high in the SEEM model as it uses Neighbour Discovery (ND) packet, Neighbour Collection (NC) packet and Neighbour Collection Reply (NCR) packet in the routing protocol. The ND packet is broadcast in network to know the neighbouring nodes of every node. Once all the nodes identify their neighbouring nodes, the base station node broadcasts NC packets in order to collect the neighbour's information of each node gathered during the previous broadcasting. The sensor nodes acknowledge to the NC packet by sending the neighbour collection reply packet to the base station. They SEEM model justifies the security without using the crypto system mechanism in the routing protocol.

## III.PROPOSED SYSTEM

In this paper we proposed a novel design end to end routing protocol for finding shortest path and also provide authentication of communication entities in the network. After completion of authentication process the group key manager will generate polynomial equation and also generate six points. The group key manager will send any three points to individual user and using those points each user will generate secret key. Using this secret session key each user will perform the encryption and decryption of transferred message. Before performing encryption and decryption process we can find shortest route by using end to end routing protocol. After that the sender will encrypt message and convert into cipher format. The completion of encryption process the sender will send that cipher format data to destination node through the path. The destination node will retrieve that data and perform the decryption process. By performing decryption process the destination node will get original message. The implementation procedure of user's authentication is as follows.

### *A. Users Authentication:*

In this module each user is send request for connection to group key manager and group key manager will accept request send universal key ($U_i$) to individual users. Before sending universal key the group key manager also generate point D for calculating distance of each node. Each user will retrieve universal key and generate random nonce ($R_i$). This random nonce will send to group key manager within format of shared points. The generation of shred points is as follow.

$$q_i = R_i / U_i$$
$$r_i = R_i \% U_i$$

Each user will take q, r values and generate those values within format of shared points (q, r), take that shared point and send to group key manager. The group key manager will get shared points of all users and generate random nonce of each user by using following formula.

$$R_i = q_i * U_i + r_i$$

After generating all random nonce of each user, the group key manager will generate random secret points of individual users and send those points to each user. Before sending those points the group key manager will xor based secret points($P_i$) and send those xor based points to individual users. The generation of xor based secret points is as follows.

$$P_i = (x_i \circledR R_i, y_i \circledR R_i)$$

In the group member will retrieve xor secret points and get the original secret points ($x_i$, yi) by applying xor operation. Each group member or user takes the secret point, id, universal key and random nonce values and generate authentication code. After generating authentication code each user will send that code to group key manager. The generation of authentication code is as follows.

$$Auth_i = H(id \mid R_i \mid U_i \mid P_i)$$

The group key manager will retrieve each user or group member authentication code and verify by using values of id, universal key, random nonce and secret point. If the user are verified successfully the group key manager will send status to each user. After completion of verification process the group key manger will generate six points for generation of secret key.

***B. Group key generation process:***

In this module the group key manager will generate group key for all users and also use that key for encryption of broad casting message. The implementation process of group key generation is as follows.

1. The group key manager will choose two random numbers and generate one secret key.

2. After generating those values the group key manager will generate polynomial equation is as follows.

$F(x) = \text{secret key} + a_0x + a_1x^2$

Here $a_0$, a1 and secret key are generated randomly.

3. After completion of polynomial equation we can divide secret key into six parts. Where any three subsets will again reconstruct secret key.

After dividing six parts the server will send any three subsets ($x_0$, y0), ($x_1$, y1) and ($x_2$, y2) to individual user.

***C. Generation of secret key by users:***

In this module each user will retrieve the subset points and get the same secret key for all users. The generation of secret key can be done by using three subset points and again reconstruct the polynomial equation. The reconstruction of polynomial equation is as follows.

$L_0 = (x\text{-}x_0/x_0\text{-}x_1)*(x\text{-}x_2/x_0\text{-}x_2)$

$L_1 = (x\text{-}x_0/x_1\text{-}x_0)*(x\text{-}x_2/x_1\text{-}x_2)$

$L_2 = (x\text{-}x_0/x_2\text{-}x_0)*(x\text{-}x_1/x_2\text{-}x_1)$

By using those values we can reconstruct polynomial equation by using following equation.

$$F(x) = \Sigma_{j=0}^{2} y_j.l_j(x)$$

After using that equation we can get original polynomial equation and get the secret key. After that the sender will choose the destination node id and send that id to group key manager. By using those ids of sender and receiver the group key manager will find out shortest route by calculating shortest distance between nodes or users or group members.

***D. Generation of distance matrix and finding Shortest Routing:***

In this module the group key manager will generate distance matrix and finding shortest route. The implementation process of distance matrix is as follows.

1. The group key manager will get all nodes of distance points and using those points we can generate distance matrix.

2. Take the each node distance points and calculate difference between each node put into matrix format. This process will repeat until completion of all nodes distance.

3. The distance of each node to other node is as follow.

$$d_i = (x1\text{-}x2) + (y1 - y2)$$

4. Finding distance source node to other nodes by using following formula

```
int max=0;

int min=di;

if (max<min)

  {
  Max=min;
}
```

5. After finding distance of each node we can arrange the path from source node to destination node.

6. So that the data send through path and reached the destination node.

After finding the path source node will transfer the data through path to destination node. Before sending data to destination node the source node will encrypt the data and transfer to destination node. The implementation procedure encryption and decryption is as follows.

***E. Encryption Process:***

In this module the sender node will enter transferred message and convert that message to unknown format. By converting plain format data into unknown format is known as encryption process. The implementation procedure of encryption process is as follows.

1. The sender node will take message and key as input of encryption process.

2. The sender node gets single character from message and converts into decimal value.

3. Take the decimal value and key perform the xor operation until message length is completed.

4. After completion of xor operation take the each decimal value and convert into eight bit binary format.

5. Take the each eight bit binary data and partition into equal parts.

6. Take those equal parts and reverse those binary partitions. Performing this reverse process until the message binary bits of data is completed.

7. Take those binary reverse bits and generate 32 * 32 matrix format.

8. Take that matrix and perform circular rotation from outer circle to inner circle.

9. After completion of circular rotation read each eight bit binary format and convert into decimal value. This process continues until all matrix data is completed.

Take those decimal values as cipher format data and send to destination node through the path. The destination node will retrieve cipher format data and convert into plain format data by performing decryption process. The implementation process of decryption is as follows.

***F. Decryption Process:***

In this module the destination node will perform decryption process for converting cipher format data into plain format.

1. The destination node will take cipher format data and key as input to decryption process.
2. The destination node takes each decimal value from cipher data and converts into eight bit binary format data.

3. Take those binary format data and generate 32 * 32 matrix format.

4. Take those matrix format data and perform reverse circular rotation from outer circle to inner circle.

5. After completion of circle rotation process take each eight bit binary format data and performing equal sub partition.

6. Take those partitions binary data and perform the reverse process of both sub parts.

7. After completion of reverse process take each eight bit binary format data and convert into decimal format until completion of cipher binary format data.

8. Take decimal value and key perform the xor operation between them until completion of all decimal values.

9. Take the xor data and convert into character format it will get plain format message.

By implementing those concepts we can improve the network efficiency and also provide more security of transferring message.

## IV. CONCLUSIONS

Our proposed system we are implementing a novel design protocol for performing authentication and key generation process. It can also implement concepts for finding shortest route from source node to destination node. In this paper we can also implement the concepts data encryption and decryption process. The authentication of users or group members can be done by group key manager and send that status to each group member. After that the group key manager will generate secret key and send that key to all group members. Each group member or user retrieve group key and send the source node, destination node to group key manager. The group key manager will retrieve source node and destination node, using those nodes ids the group key manager will calculate shortest route from source node to destination node. After finding the shortest route the group key manager send that path to both users. Both users are retrieve path and source node will encrypt the transferred message. After converting plain format data into cipher format data can be send to specified destination node. The destination node will retrieve the cipher format and perform the decryption process, it will get original plain format message. So that by proposing those concepts we can provide more security of transferring message and also improve network efficiency.

## REFERENCES


[1] I.F. Akyildiz et al, W.Su, Y.Sankara subramaniam, E.Cayirci "Wireless sensor networks: a survey", Computer Networks, Vol. 38, pp. 393- 422, March 2002

[2] K.Akkaya, M younis "A survey on routing protocols for wireless sensor networks" Ad Hoc Networks 3 (2005), pp 325-345, 2005.

[3] M. L. Das, "Two-factor user authentication in wireless sensor networks," *IEEE Trans. Wireless Commun.*, vol. 8, no. 3, pp. 1086–1090, Mar. 2009.

[4] L. Eschenauer and V. D. Gligor, "A key-management scheme for distributed sensor networks," in *Proc. ACM Conf. CCS*, 2002, pp. 41–47.

[5] L. Harn and C. F. Hsu, "Predistribution scheme for establishing group keys in wireless sensor networks," *IEEE Sensors J.*, vol. 15, no. 9,

[6] pp. 5103–5108, Sep. 2015.

[7] W. Gu, N. Dutta, S. Chellappan, and X. Bai, "Providing end-to-end secure communications in wireless sensor networks," *IEEE Trans. Netw. Service Manage.*, vol. 8, no. 3, pp. 205–218, Sep. 2011.

[8] "21 ideas for the 21st century", Business Week, Aug. 30 1999, pp. 78-167.
[9] S.K. Singh, M.P. Singh, and D.K. Singh, "A survey of Energy-Efficient Hierarchical Cluster-based Routing in Wireless Sensor Networks", International Journal of Advanced Networking and Application (IJANA), Sept.–Oct. 2010, vol. 02, issue 02, pp. 570–580.
[10] S.K. Singh, M.P. Singh, and D.K. Singh, "Energy-efficient Homogeneous Clustering Algorithm for Wireless Sensor Network", International Journal of Wireless & Mobile Networks (IJWMN), Aug. 2010, vol. 2, no. 3, pp. 49-61.
[11] Jun Zheng and Abbas Jamalipour, "Wireless Sensor Networks: A Networking Perspective", a book published by A John & Sons, Inc, and IEEEE, 2009.
[12] Luis Javier García Villalba, Ana Lucila Sandoval Orozco, Alicia Triviño Cabrera, and Cláudia Jacy Barenco Abbas, "Routing Protocol in Wireless Sensor Networks", Sensors 2009, vol. 9, pp. 8399- 8421.
[13] E. Zanaj, M. Baldi, and F. Chiaraluce, "Efficiency of the Gossip Algorithm for Wireless Sensor Networks", In Proceedings of the 15th International Conference on Software, Telecommunications and Computer Networks (SoftCOM), Split–Dubrovnik, Croatia, September, 2007.