ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

An Efficient Secure End to End Routing Protocol Based on Authentication and Encryption for wireless Sensor Network

Telugu Ramaraju
Final M.Tech Student,
Dept of CSE,
Sarada Institute of Science Technology and Management (SISTAM),
Srikakulam, Andhra Pradesh.

Chintada Sunil Kumar
Assistant Professor,
Dept of CSE,
Sarada Institute of Science Technology and Management (SISTAM),
Srikakulam, 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:
Cryptography, routing, security, network security, wireless sensor network.

I. INTRODUCTION:

Wireless sensor network (WSN) is widely considered as one of the most important technologies for the twenty-first century [1]. 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 [2,3]. 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 [4]. 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

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

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. 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 analyze 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. (Size 10 & Normal)This document is a template. An electronic copy can be downloaded from the conference website. For questions on paper guidelines, please contact the conference publications committee as indicated on the conference website. Information about final paper submission is available from the conference website.

II. RELATED WORK:

Security issues in ad-hoc networks are similar to those in sensor networks and have been well enumerated in the literature [5], [6], but the defense mechanisms developed for ad-hoc networks are not directly applicable to sensor networks. There are several reasons for why this is so, but they all relate to the differences between sensor and ad-hoc networks enumerated in the previous section. Some ad-hoc network security mechanisms for authentication and secure routing protocols are based on public key cryptography [7], [8], [9], [10], [11], [12], [13], [14]. Public key cryptography is too expensive for sensor nodes. Security protocols for sensors networks must rely exclusively on efficient symmetric key cryptography. Secure routing protocols for ad-hoc networks based on symmetric key cryptography have been proposed [15], [16], [17], [18].

These protocols are based on source routing or distance vector protocols and are unsuitable for sensor networks. They are too expensive in terms of node state and packet overhead and are designed to find and establish routes between any pair of nodes—a mode of communication not prevalent in sensor networks. Marti et al. [19] and Buchegger and Boudec [20] consider the problem of minimizing the effect of misbehaving or selfish nodes on routing through punishment, reporting, and holding grudges. These applications of these techniques to sensor networks are promising, but these protocols are vulnerable to blackmailers. Perrig et al. present two building block security protocols optimized for use in sensor networks, SNEP and TESLA. SNEP provides confidentiality, authentication, and freshness between nodes and the sink, and TESLA provides authenticated broadcast.

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.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

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.

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,y_i) 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.

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

$F(x) = \text{secret key} + a_0 x + a_1 x^2$

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,y_0), (x_1,y_1) and (x_2,y_2)to individual user.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

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.

$L_0 = (x-x_0/x_0-x_1)*(x-x_2/x_0-x_2)$

$L_1 = (x-x_0/x_1-x_0)*(x-x_2/x_1-x_2)$

$L_2 = (x-x_0/x_2-x_0)*(x-x_1/x_2-x_1)$

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.

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.

$$d_i = (x1-x2) + (y1 - y2)$$

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.

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.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

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.

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.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

So that by proposing those concepts we can provide more security of transferring message and also improve network efficiency.

REFERENCES:

[1].“21 ideas for the 21st century”, Business Week, Aug. 30 1999, pp. 78-167.

[2].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.

[3].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.

[4].Jun Zheng and Abbas Jamalipour, “Wireless Sensor Networks: A Networking Perspective”, a book published by A John & Sons, Inc, and IEEEE, 2009.

[5].L. Zhou and Z. Haas, “Securing ad hoc networks,” IEEE Network Magazine, vol. 13, no. 6, November/December 1999.

[6]. F. Stajano and R. J. Anderson, “The resurrecting duckling: Security issues for ad-hoc wireless networks,” in Seventh International Security Protocols Workshop, 1999, pp. 172–194.

[7]. J. Hubaux, L. Buttyan, and S. Capkun, “The quest for security in mobile ad hoc networks,” in Proceedings of the ACM Symposium on Mobile Ad Hoc Networking and Computing (MobiHOC 2001), 2001.

[8]. J. Kong, P. Zerfos, H. Luo, S. Lu, and L. Zhang, “Providing robust and ubiquitous security support for mobile ad-hoc networks,” in ICNP, 2001, pp. 251–260.

[9]. M. G. Zapata, “Secure ad-hoc on-demand distance vector (SAODV) routing,” IETF MANET Mailing List, Message-ID: 3BC17B40.BBF52E09@nokia.com, Available at ftp://manet.itd.nrl.navy.mil/pub/manet/2001-10.mail, October 8, 2001.

[10] H. Luo, P. Zefros, J. Kong, S. Lu, and L. Zhang, “Self-securing ad hoc wireless networks,” in Seventh IEEE Symposium on Computers and Communications (ISCC ’02), 2002.

[11]. J. Binkley and W. Trost, “Authenticated ad hoc routing at the link layer for mobile systems,” Wireless Networks, vol. 7, no. 2, pp. 139–145, 2001.

[12]. B. Dahill, B. N. Levine, E. Royer, and C. Shields, “A secure routing protocol for ad-hoc networks,” Electrical Engineering and Computer Science, University of Michigan, Tech. Rep. UM-CS-2001-037, August 2001.

[13]. J. Kong, H. Luo, K. Xu, D. L. Gu, M. Gerla, and S. Lu, “Adaptive security for multi-layer ad-hoc networks,” Special Issue of Wireless Communications and Mobile Computing, Wiley Interscience Press, 2002.

[14]. Y.-C. Hu, D. B. Johnson, and A. Perrig, “SEAD: Secure efficient distance vector routing for mobile wireless ad hoc networks,” in Proceedings of the 4th IEEE Workshop on Mobile Computing Systems and Applications (WMCSA 2002), June 2002, pp. 3–13.

[15]. Y.-C. Hu, A. Perrig, and D. B. Johnson, “Ariadne: A secure on-demand routing protocol for ad hoc networks,” Department of Computer Science, Rice University, Tech. Rep. TR01-383, December 2001.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

[16]. S. Basagni, K. Herrin, E. Rosti, and D. Bruschi, "Secure pebblenets," in ACM International Symposium on Mobile Ad Hoc Networking and Computing (MobiHoc 2001), October 2001, pp. 156–163.

[17]. P. Papadimitratos and Z. Haas, "Secure routing for mobile ad hoc networks," in SCS Communication Networks and Distributed Systems Modeling and Simulation Conference (CNDS 2002), January 2002.

[18]. S. Marti, T. J. Giuli, K. Lai, and M. Baker, "Mitigating routing misbehavior in mobile ad hoc networks," in Sixth annual ACM/IEEE Internation Conference on Mobile Computing and Networking, 2000, pp. 255–265.

[19]. S. Buchegger and J.-Y. L. Boudec, "Nodes bearing grudges: Towards routing security, fairness, and robustness in mobile ad hoc networks," in Proceedings of the Tenth Euromicro Workshop on Parallel, Distributed and Network-based Processing. Canary Islands, Spain: IEEE Computer Society, January 2002, pp. 403–410.

[20] A. Perrig, R. Szewczyk, V. Wen, D. Culler, and J. Tygar, "SPINS: Security protocols for sensor networks," in Proceedings of Mobile Networking and Computing 2001, 2001.

BIOGRAPHIES:

Telugu Ramaraju is student in M.tech (CSE) in Sarada Institute of Science Technology and Management, Srikakulam. He has received her B.tech (CSE) from Sri Vaishnavi College of Engineering, Singupuram, and Srikakulam. His interesting areas are data mining, network security and cloud computing

Chintada Sunil Kumar working as a Asst Professor of CSE in Sarada Institute of Science, Technology and Management (SISTAM), Srikakulam, Andhra Pradesh. He received his M.Tech (CSE) from Jntuk, Kakinada. Andhra Pradesh. His interest research areas are Database management systems, Computer Architecture, Image Processing, Computer Networks, Distributed Systems. He published 4 international journals and he was attended number of conferences and workshops.