An Approach for Secure Group Communication Mechanism in Wireless Sensor Networks

[1]Shiv Prakash Kumar, [2]Dr Mamatha T
[1]Research Scholar, [2]Associate professor
[1]Department of Electronics & Communication Engineering
[2]department of CSE
[1]B.R. A. Bihar University, Muzaffarpur, Bihar, India
[2]Maulana Azad Engineering College (A.K. University), Patna, Bihar, India

***Abstract*:** One of the most important tasks of the sensor nodes is systematic collection of data and transmits gathered data to a distant base station (BS). Clustering tree has proven an effective approach for organizing a large scale WSN into connected groups increasing the lifetime and the reliability of such networks. Distance of the nodes from the base station and inter-node distances can have a high influence on saving energy and extending the network lifetime. In this process, a secure hash key generation method based attacker identification and data transmission in WSN is proposed. This optimizes clustering process by considering the energy, distance of each node. This feature will have a great effect in prolonging the network lifetime as it reduces the amount of energy wasted on replacing the node. To the best of our knowledge, few routing schemes have for delay less performance into consideration. Simulation result shows the proposed system decreases data collection delay, attacker free network and energy consumption compared with the existing schemes. In this work Propose a secure hash key generation method for providing attacker free network. This light-weight, one-way, cryptographic hash algorithm is suggested with a target to produce a hash-digest with fixed and relatively small length for such an energy-starved wireless network.

***Index Terms* –Group communication system, wireless sensor network, hash key generation.**

I. INTRODUCTION

Due to recent technological advances, the manufacturing of small and low cost sensors became technically and economically feasible. The sensing electronics measure ambient conditions related to the environment surrounding the sensor and transform them into an electric signal.

Processing such a signal reveals some properties about objects located and/or events happening in the vicinity of the sensor. A large number of these disposable sensors can be networked in many applications that require unattended operations. A Wireless Sensor Network (WSN) contains hundreds or thousands of these sensor nodes. These sensors have the ability to communicate either among each other or directly to an external base station (BS). A greater number of sensors allows for sensing over larger geographical regions with greater accuracy. Sensor nodes are usually scattered in a sensor field, which is an area where the sensor nodes are deployed. Sensor nodes coordinate among themselves to produce high-quality information about the physical environment. Each sensor node bases its decisions on its mission, the information it currently has, and its knowledge of its. Taking into account the reduced capabilities of sensors, the communication with the sink could be initially conceived without a routing protocol. With this premise, the flooding algorithm stands out as the simplest solution. In this algorithm, the transmitter broadcasts the data which are consecutively retransmitted in order to make them arrive at the intended destination. However, its simplicity brings about significant drawbacks.

Firstly, an implosion is detected because nodes redundantly receive multiple copies of the same data message. Then, as the event may be detected by several nodes in the affected area, multiple data messages containing similar information are introduced into the network. Moreover, the nodes do not take into account their resources to limit their functionalities. One optimization relies on the gossiping algorithm. Gossiping avoids implosion as the sensor transmits the message to a selected neighbor instead of informing all its neighbors as in the classical flooding algorithm. However, overlap and resource blindness are still present.

Furthermore, these inconveniences are highlighted when the number of nodes in the network increases. Due to the deficiencies of the previous strategies, routing protocols become necessary in wireless sensor networks. One of the main limitations is the identification of nodes. Since wireless sensor networks are formed by a significant number of nodes, the manual assignation of unique identifiers becomes infeasible. The use of potentially unique identifier such as the MAC (Medium Access Control) address or the GPS coordinates is not recommended as it forces a significant payload in the messages. However, this drawback is easily overcome in wireless sensor networks since an IP address is not required to identify the destination node of a specific packet. In fact, attribute-based addressing fits better with the specificities of wireless sensor networks. In this case, an attribute such as node location and sensor type is used to identify the final destination. Once nodes are identified, routing protocols are in charge of constructing and maintaining routes between distant nodes. The different ways in which routing protocols operate make them appropriate for certain applications.

II. EXISTING SYSTEM

In existing system an improved key distribution mechanism for large-scale hierarchical wireless sensor network. Due to their expensive energy consumption and hardware requirements, asymmetric key based cryptographies are not suitable for resource-constrained wireless sensors. Several symmetric-key pre-distribution protocols have been investigated recently to establish secure links between sensor nodes, but most of them are not scalable due to their linearly increased communication and key storage overheads. Furthermore, existing protocols cannot provide sufficient security when the number of compromised nodes exceeds a critical value. Wireless sensor networks are often deployed in hostile environments and operated on an unattended mode. In order to protect the sensitive data and the sensor readings, secret keys should be used to encrypt the exchanged messages between communicating nodes. Due to their expensive energy consumption and hardware requirements, asymmetric key based cryptographies are not suitable for resource-constrained wireless sensors. Several symmetric-key pre-distribution protocols have been investigated recently to establish secure links between sensor nodes, but most of them are not scalable due to their linearly increased communication and key storage overheads. Furthermore, existing protocols cannot provide sufficient security when the number of compromised nodes exceeds a critical value.

III. PROPOSED SYSTEM

Propose a secure hash key generation method for providing attacker free network. This light-weight, one-way, cryptographic hash algorithm is suggested with a target to produce a hash-digest with fixed and relatively small length for such an energy-starved wireless network. The primary focus is making the algorithm light-weight so that upon using it in application of network like WSN, the nodes can successfully run the algorithm with low energy. It is suggested that such algorithm must fulfill all the basic properties such as pre-image resistance, collision resistance of a one-way hash function.A cluster tree method which is depends on node position as well as energy is proposed. The cluster head act as a group controller security mechanism of other normal nodes.

A. SYSTEM ARCHITECTURE

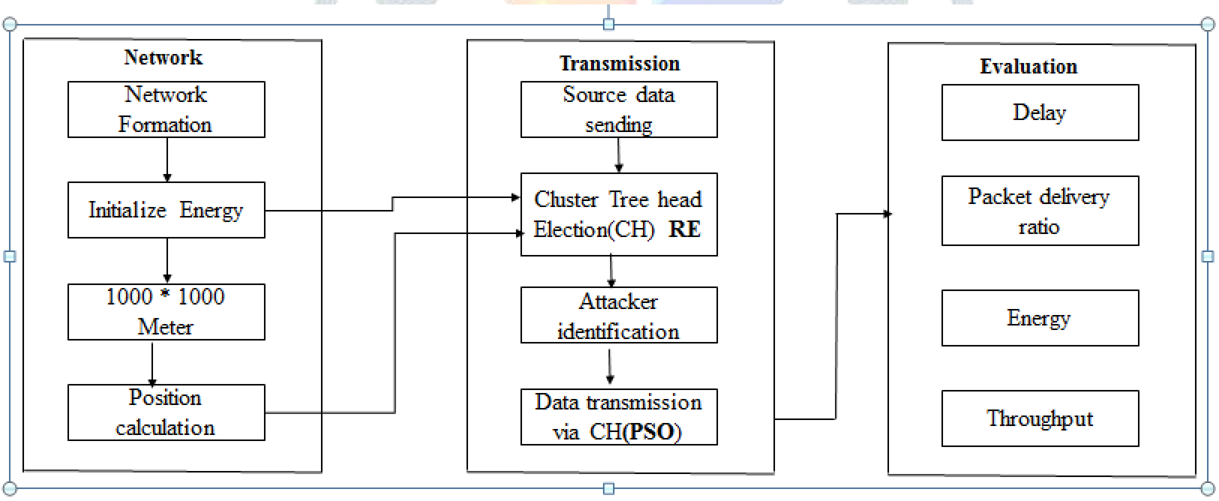

Fig 1. System Architecture

B. NETWORK FORMATION

Wireless networks are composed of a number of sensor nodes that deployed in a field. Radio channel we use two ray ground. We deploy 100 numbers of nodes, and the transmission range is 1000 meters. We consider File transfer protocol (FTP) and randomly choose different source-destination connections. Our network contains source, cluster, volunteer and destination nodes. Every source data is in bytes format.

C. CLUSTER SEPARATION

100 nodes are randomly deployed in that region. After the normal nodes are deployed, the base station node is fixed and all the other nodes are in random mobility model. All the nodes have the same energy while network deployment. The cluster head is elected depending upon the residual energy of the node. The node which has highest energy is taken as cluster head and all the transmission between the nodes are done via the layer head.

D. ATTACKER IDENRIFICATION AND SECURITY

Security will be provided by using secure hash key generation method in wireless sensor networks. Cluster head is act as a group controller who have the secure hash key. The attacker will be identified and block listed from the network. We also maintained route table for monitoring activities of every node transmission.

E. DATA TRANSMISSION

Data transmission is done by using TCP connection protocol. The node is selected based upon the energy and position of the node. If the node is nearest to the destination then the data directly sent to that destination else it sent the data via neighbor.

IV. RESULTS

The graphs shows the energy loss during the transmission. The security algorithm uses less energy which will maximize the life of a sensor node.

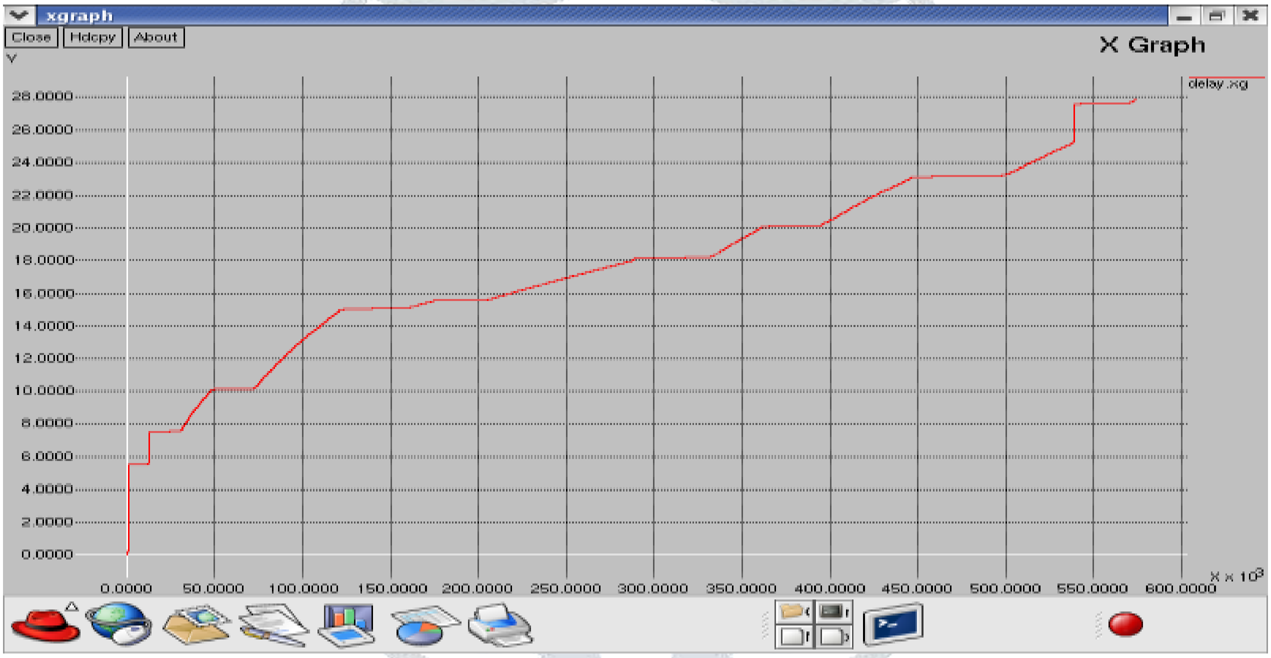

Fig. 2. Delay

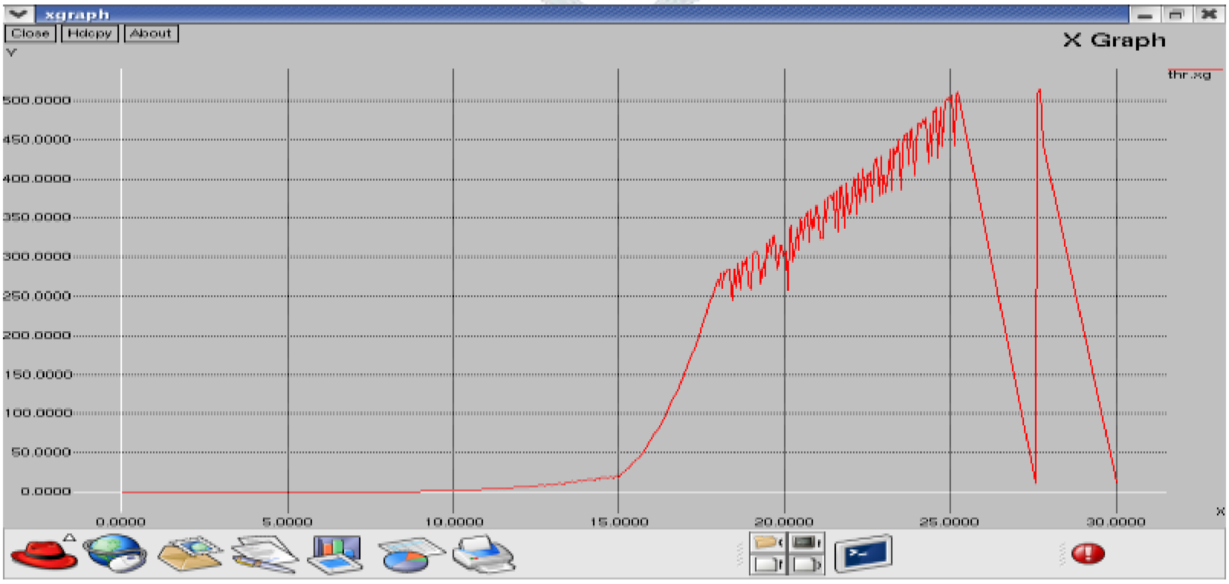

Fig. 3 Throughput

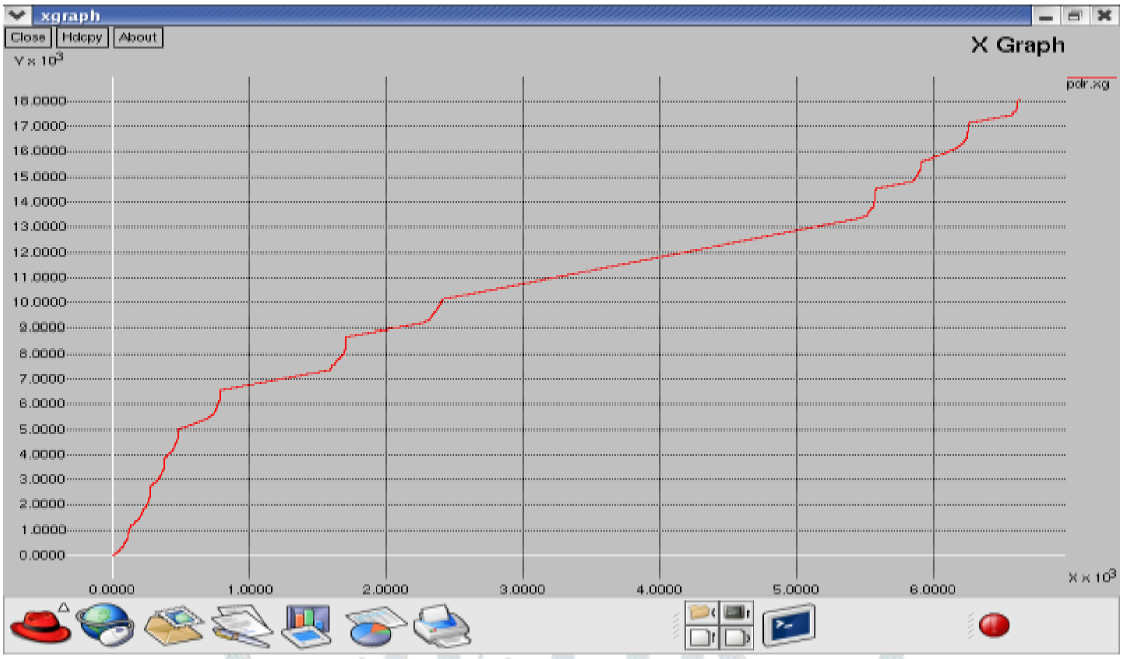

Fig. 4 Cluster Node Energy

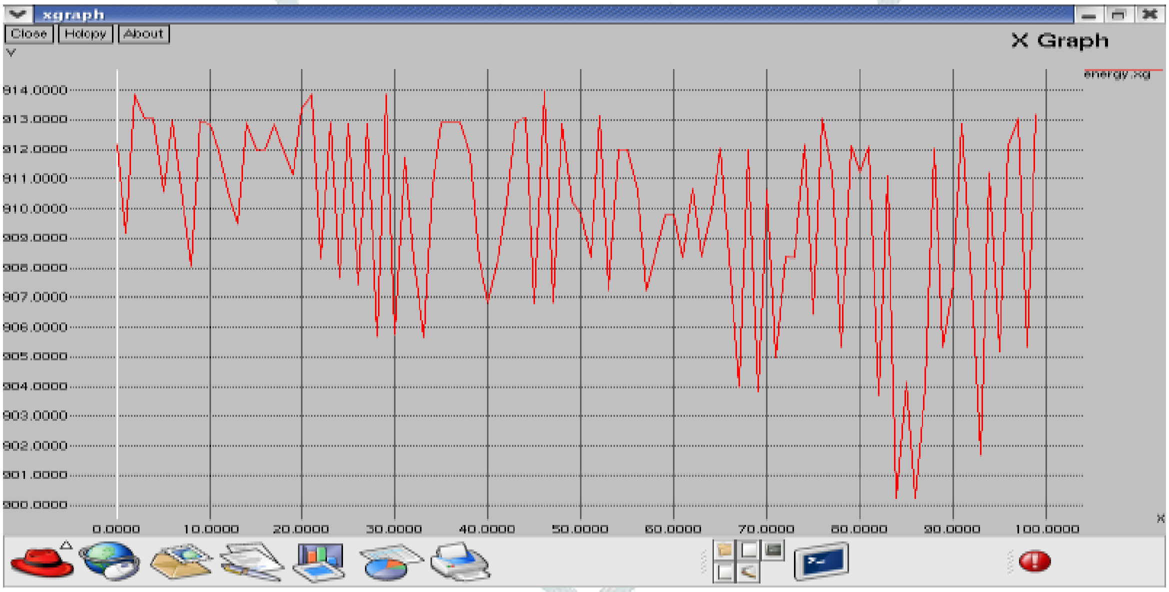

Fig.5 Energy

V. CONCLUSION AND FUTURE WORK

A. Conclusion

- Thus our proposed process attain attacker free environment using secure hash generation in wireless sensor networks
- Simulation result shows our proposed system provides better network lifetime than other protocols.

B. FUTURE WORK

In future, we will implement our process with some more security aspects. For achieving this we will implement one way hash function encryption and decryption for the packets for more secure transmission.

REFERENCES

1. A. Mainwaring, J. Polastre, R. Szewczyk, D. Culler, and J. Anderson, “Wireless sensor networks for habitat monitoring,” WSNA ’02: International Workshop on Wireless Sensor Networks and Applications, pp. 88–97, 2002.
2. Z. Benenson, N. Gedicke, and O. Raivio, “Realizing robust user authentication in sensor networks,” Real-World Wireless Sensor Networks (REALWSN), June 2005.
3. H.-R. Tseng, R.-H. Jan, and W. Yang, “An improved dynamic user authentication scheme for wireless sensor networks,” Global Telecommunications Conference, GLOBECOM ’07. IEEE, pp. 986–990, November 2007.
4. L. Li, J. Li, L. Tie, and J. Pan, “Ackds: An authenticated combinatorial key distribution scheme for wireless sensor networks,” software Engineering, Artificial intelligence, Networking, and Parallel/distributed Computing, SNPD, pp. 262–267, December 2007.
5. Y. H. Kim, H. Lee, and D. H. Lee, “A key distribution scheme for wireless sensor networks,” Pervasive Computing and Communications, Sixth Annual IEEE International Conference on, vol. 17, pp. 572 – 577, March 2008.
6. R. D. Pietro, P. Michiardi, and R. Molva, “Confidentiality and integrity for data aggregation in wsn using peer monitoring,” Security and Communication Networks, vol. 2, pp. 181–194, Jan 2009.
7. H. bin Wang, Z. Yuan, and C. dong Wang, “Intrusion detection for wireless sensor networks based on multi-agent and refined clustering,” International Conference on Communications and Mobile Computing, vol. 3, pp. 450–454, December 2009.
8. Z. Du, K. Wang, and L. Zhou, “Efficient broadcast authentication in wireless sensor networks,” IEEE Asia-Pacific Services Computing Conference, pp. 187–192, 2008.
9. B. Lejla, M. Nele, S. Kazuo, P. Bart, and V. Ingrid, “Low-cost elliptic curve cryptography for wireless sensor networks,” Lecture notes in computer science ISSN 0302-9743, vol. 4357, pp. 6–17, 2006.
10. Y. Cheng and D. Agrawal, “An improved key distribution mechanism for large-scale hierarchical wireless sensor networks,” Ad Hoc Networks (Elsevier), vol. 5, no. 1, pp. 35–48, 2007.
11. D. Huang, M. Mehta, D. Medhi, and L. Harn, “Location-aware key management scheme for wireless sensor networks,” 2nd ACM workshop on Security of ad hoc and sensor networks SASN 04, pp. 29–42, 2004.
12. W. R. Heinzelman, A. Chandrakasan, and H. Balakrishnan, “Energy efficient communication protocol for wireless microsensor networks,” 3rd Annual Hawaii International Conference on System Sciences, p. 8020-8026, January 2000.
13. S. Zhu, S. Setia, and S. Jajodia, “Leap: efficient security mechanisms for large-scale distributed sensor networks,” 10th ACM conference on Computer and communications security. New York, NY, USA: ACM Press, pp. 62–72, 2003.
14. L. Zhang, Z. Hu, Y. Li, and X. Tang, “Grouping-based clustering routing protocol in wireless sensor networks,” Wireless communications, networking and mobile computing, Wicom, pp. 2452–2455, 2007.
15. L. Li, J. Li, L. Tie, and J. Pan, “Ackds: An authenticated combinatorial key distribution scheme for wireless sensor networks,” the software Engineering, Artificial intelligence, Networking, and Parallel/distributed Computing, SNPD, pp. 262–267, 2007.
16. X. Zou, B. Ramamurthy, and S. S. Magliveras, Secure Group Communications over Data Networks. Springer, 2005.
17. Y. Wang and B. Ramamurthy, “Group rekeying schemes for secure group communication in wireless sensor networks,” Communications, ICC apos, pp. 3419–3424, June 2007.
18. M. Tubaishat, J. Yin, B. Panja, and S. Madria, “A secure hierarchical model for sensor network,” SIGMOD Rec., vol. 33, no. 1, pp. 7–13, 2004.
19. N. Thepvilojanapong, Y. Tobe, and K. Sezaki, “A proposal of secure group communication for wireless sensor networks,” The 23th Computer Security (CSEC) Group Meeting, IPSJ, Tokyo, Japan, pp. 47–52, December 2003.
20. A. DAS and I. Sengupta, “An effective group-based key establishment scheme for large-scale wireless sensor networks using bivariate polynomials,” Communication Systems Software and Middleware and workshops, pp. 9–16, 2008