Dynamic Energy Based Data Transmission with Secure Authentication in Wireless Sensor Network

P. Ramachandran
Assistant Professor, Dept. of Computer Science and Engineering, Chennai Institute of Technology, Chennai, Tamil Nadu, India.

V. Muthukumar
Dept. of Computer Science and Engineering, Chennai Institute of Technology, Chennai, Tamil Nadu, India.

S. Aarthi
Dept. of Computer Science and Engineering, Chennai Institute of Technology, Chennai, Tamil Nadu, India.

Abstract – Recently the wireless Sensor Network (WSN) is an emerging technology. And it shows effective usage and applications for the world, such as army, communication and everything. etc., Sensor nodes are typically powered by batteries with a limited lifetime and, even when additional energy can be harvested from the external environment (e.g., through solar cells or piezo-electric mechanisms), it remains a limited resource to be consumed judiciously. Efficient energy management is thus a key requirement for a credible design of a wireless sensor network. Most energy management strategies proposed in the literature assume that data acquisition consumes significantly less energy than their transmission. In this paper introduce effective energy based algorithm to develop the data transmission process without any delay and data losses efficiently. For achieving this technique add the higher security to each and every transmission. It helps to reduce the illegal accessing and time delay on wireless sensor network (WSN).

Index Terms – Wireless Sensor Network, Piezo-Electronic Mechanism.

1. INTRODUCTION

Wireless Sensor Networks (WSN) are emerging as both an important new tier in the IT ecosystem and a rich domain of active research involving hardware and system design, networking, distributed algorithms, programming models, data management, security and social factors [1], [2], [3]. The basic idea of sensor network is to disperse tiny sensing devices; which are capable of sensing some changes of incidents/parameters and communicating with other devices, over a specific geographic area for some specific purposes like target tracking, surveillance, environmental monitoring etc. Today's sensors can monitor temperature, pressure, humidity, soil makeup, vehicular movement, noise levels, lighting conditions, the presence or absence of certain kinds of objector substances, mechanical stress levels on attached objects, and other properties [4]. In case of wireless sensor network, the communication among the sensors is done using wireless transceivers. However, while the routing strategies and wireless sensor network modeling are getting much preference, the security issues are yet to receive extensive focus. In this paper explore the security issues and challenges for next generation wireless sensor networks and discuss the crucial parameters that require extensive investigations.

1.1. Cryptography

The encryption-decryption techniques devised for the traditional wired networks are not feasible to be applied directly for the wireless networks and in particular for wireless sensor networks. WSNs consist of tiny sensors which really suffer from the lack of processing, memory and battery power [6], [7], [8], [9]. Applying any encryption scheme requires transmission of extra bits, hence extra processing, memory and battery power which are very important resources for the sensors' longevity. Applying the security mechanisms such as Encryption could also increase delay, jitter and packet loss in wireless sensor networks [10]. Moreover, some critical questions arise when applying encryption schemes to WSNs like, how the keys are generated or disseminated. How themes are managed, revoked, assigned to a new sensor added to the network or renewed for ensuring robust security for the network. As minimal (or no) human interaction for the sensors, is a fundamental feature of wireless sensor networks, it becomes an important issue how the keys could be modified time to time for encryption. Adoption of pre-loaded keys or embedded keys could not be an efficient solution.

2. RELATED WORK

2.1. Resources Constraints

Because of size, form factor and cost considerations, wireless sensor networks suffer from severe resource constraints, such as communication bandwidth and range, computation power, memory and energy. Therefore, WSN has a demand of the energy-efficiency of key establishment protocols. Traditional key establishment mainly includes public key cryptography which requires heavy computations. New techniques should be developed for the special Conditions of WSN.

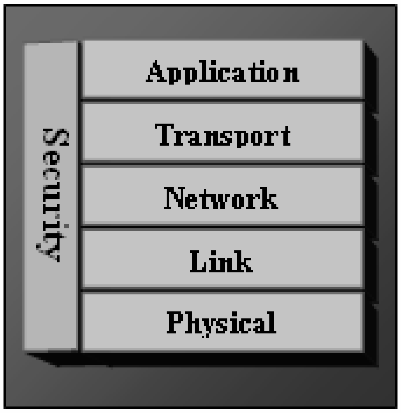


Figure 1 Layers of data transmission

2.2. Secure Path Key Agreement

Considering that the sensor nodes are dispersed when they are deployed, nodes sometimes have to communicate others by the routing on multi-hops of ad hoc network. International Journal of Network Security & Its Applications (IJNSA), Vol 1, No 2, July 2009neighbored nodes are to agree on secret key with each other (We call it "path key agreement"),hey have to send their secret respective message to each other over the multi-hop media. Especially if the network is deployed in a hostile environment, the process of path key agreement should not expose any sensitive information to the other parties even in a supposed secure channel.

2.3. Secure Group Communication

To conserve power, intermediate network nodes should aggregate results from individual sensors. Aggregation collects results from several sensors and calculates a smaller message that summarizes the important information from a group of sensors. For example, suppose the operator is interested in the average sensor reading for some value in the network. An inefficient way to find this would be for every sensor node to send its reading to the base station (possibly over multiple forwarding hops), and for the base station to calculate the average of all readings received. A more efficient way to collect the same information would be for intermediate nodes to forward the calculated average value of the readings they receive along with a count of the number of readings it incorporates. Each node then calculates the average for all of its descendants and only need send that value and the number of descendants to its parent. This group operation needs secure group communications.

3. SYSTEM MODEL

However, group key establishment is the bottle neck for secure group communication in WSN. The roadmap of this paper is as follows: Section 2 gives a brief overview of research background related to our scheme, including LU composition for pair wise key establishment, integrating LU composition with elliptic curve D-H for path-key establishment, and tree-based extension of LU composition for group key establishment .Section 3 illustrates the related works about this key establishment for WSN. It describes our scheme to solve the problem. Lastly, Section 5 gives some concluding remarks about this paper, as well as briefly reporting the status of this piece of research work.

Figure 2 System model of Data transmission

4. RESULT ANALYSIS

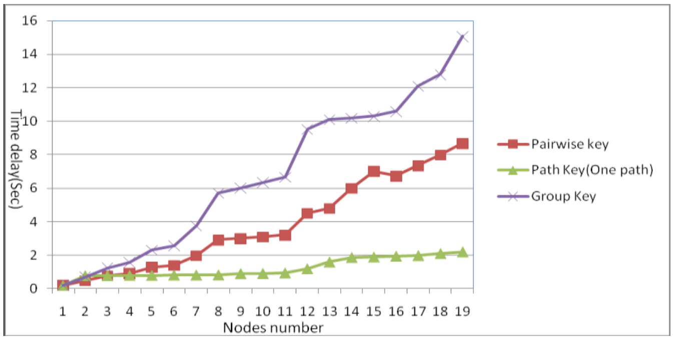
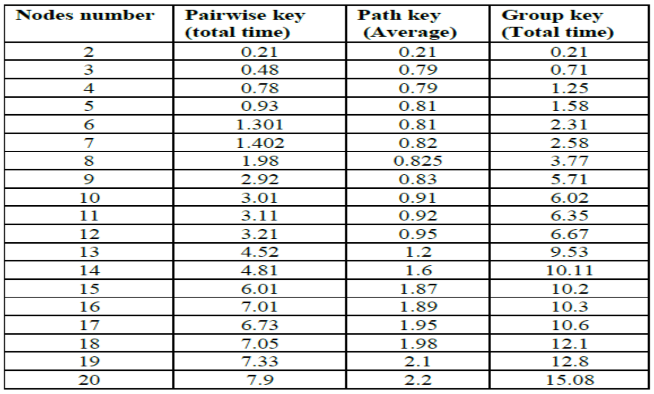


Figure 3 Data Transmission overview with various keys – Time delay & Nodes Number

Here the diagrams show data effective data transmission including various keys. Such as pair wise key, Path key (one bath) and Group key. And the views are classified into two field one Data transmission nodes number and Time delay per second. These two aspects show the effective data transmission without data losses in wireless sensor network. Using Symmetric key cryptography, both data nodes share the same key for encryption and decryption. To provide privacy, this pair-wise key needs to be kept secret. For that reason, the key must not be transmitted between nodes over the network. This technique keeps the keys secret with a greater degree. The number of iterations to be applied upon an initial state is discovered. The nodes are inserted into various iterations and other decides to apply more than 20. This generates the pair wise key length of 2k. Example 256-bit key. This factor creates highest degree of security on data transmission in wireless sensor networks.



Nodes number	Pairwise key (total time)	Path key (Average)	Group key (Total time)
2	0.21	0.21	0.21
3	0.48	0.79	0.71
4	0.78	0.79	1.25
5	0.93	0.81	1.58
6	1.301	0.81	2.31
7	1.402	0.82	2.58
8	1.98	0.825	3.77
9	2.92	0.83	5.71
10	3.01	0.91	6.02
11	3.11	0.92	6.35
12	3.21	0.95	6.67
13	4.52	1.2	9.53
14	4.81	1.6	10.11
15	6.01	1.87	10.2
16	7.01	1.89	10.3
17	6.73	1.95	10.6
18	7.05	1.98	12.1
19	7.33	2.1	12.8
20	7.9	2.2	15.08

Figure 4 Table of key generation – Pair wise key (total time), Path Key (Average), Group Key (total time).

5. CONCLUSION & FUTURE WORK

In this paper worked how the data transfer can be secured and which security mechanism used to protect the data transmission losses. To avoid the data pocket loss we introduce encryption method with various key algorithms. It shows effective data transmission is possible in wireless sensor network.

In future work to increase data transmission rate initially provided tiny delay for SMAC and AEMAC schemes. These algorithms are providing minimum delay. So it enhances the secure data transmission in wireless sensor network.

REFERENCES

[1] Arvinderpal S. Wander, Nils Gura, Hans Eberle, Vipul Gupta, and Sheueling Chang Shantz.(2005) Energy Analysis of Public Key Cryptography for Wireless Sensor Networks. In Proceedings of the Third IEEE International Conference on Pervasive Computing and Communications, pages 324– 328.

[2] Rodrigo Roman, Jianying Zhou, and Javier Lopez.(2005)On the security of wireless sensor networks.In Internet Comunications Security (WICS) Workshop, ICCSA (3) 2005, pages 681–690

[3] Yi Cheng and Dharma P. Agrawal. (2006) Energy Efficient Session Key Establishment in Wireless Sensor Networks. In PROCEEDINGS OF THE 2006 INTERNATIONAL CONFERENCE ONWIRELESS NETWORKS(ICWN'06), pages 136–142.

[4] S.K. Ghosh, R.K. Patro, M. Raina, C. Thejaswi, and V. Ganapathy. (2006) Secure groupcommunication in wireless sensor networks. 1th International Symposium on Wireless PervasiveComputing.

[5] X Dai, F Xia, Z Wang, and Y Sun. (2005)A Survey of Intelligent Information Processing in WirelessSensor Network . In International Conference on Mobile Ad-hoc and Sensor Networks, page 8.

[6] Chang Won Park, Sung Jin Choi, and Hee Yong Youn. (2005)A noble key predistribution scheme with matrix for secure wireless sensor networks. In Proc. of Computational Intelligence andSecurity - CIS'05, pages 494–499.

[7] Certicom Research. Standards for efficient cryptography, SEC 1: Elliptic Curve Cryptography. Available on the Web, http://www.secg.org/download/aid-385/sec1_final.pdf.

[8] Donggang Liu, PengNing, and Wenliang Du. (2005)Group-Based Key Pre-Distribution in Wireless Sensor Networks.In ACM WiSE05.

[9] Lijun Liao. and Mark Manulis. (2006) Tree-Based Group Key Agreement Framework for Mobile Ad-Hoc Networks. In Proceedings of the 20th International Conference on Advanced Information Networking and Applications (AINA06).

[10] SEYIT A.CAMTEPE and BULENT YENER. Key Distribution Mechanisms for Wireless Sensor Networks:a Survey. Technique Report.

[11] Haowen Chan, Adrian Perrig, and Dawn Song. (2003)Random key predistribution schemes for sensor networks. In Security and Privacy, 2003.

[12] Erdos P and Renyi A. (1959) Onrandom graphs. PublicationesMathematicae.

[13] Liu D and Ning P. (2003)Location-based pairwise key establishments for static sensor networks. InProceedings of the 1st ACM Workshop on Security of Ad Hoc and Security of Ad Hoc and SensorNetworks:USA:ACM,2003, pages 72–78.

[14] L.Eschenauer and V.D.Gligor. (2002). key-management scheme for distributed sensor networks.InProceedings of the 9th ACM Conference on Computer and Communications Security, 2002.

[15] S. Zhu, Setia S. Xu, S., and Jajodia. (2003). Establishing pairwise keys for secure commu- nicationin ad hoc networks: a probabilistic approach. In 11th IEEE International Conference on Network Protocols (ICNP03).

[16] Blom.R. (1985). An optimal class of symmetric key generation systems. In Eurocrypt, page 84. 26International Journal of Network Security & Its Applications (IJNSA), Vol 1, No 2, July 2009

[17] A. E. E. Bresson, O. Chevassut, and D. Pointcheval(2003). Mutual authentication and group keyagreement for low-power mobile devices. In Proceedings of MWCN 2003, pages 59–62. World Scientific Publishing.