Analyzing & Securing Data Transmission in Wireless Sensor Networks through Cryptography Techniques

Shahid Ishaq[1*], Rashmi Raj[2]

[1]Research Scholar, [2]Assistant Professor
Department of Electronics and Communication Engineering,
Universal Institute of Engineering & Technology, Mohali, Punjab

ABSTRACT

Wireless Sensor Networks are gaining popularity in various fields and areas. But these nodes are vulnerable as they are open networks and easily accessible. The major challenge is to have a secure data transmission between the nodes. To establish a secure transmission, we require a security scheme like a cryptographic algorithm, but this also requires a secure key distribution between nodes. The WSN's have constraints like limited area, power and memory which restrict all the categories of cryptographic algorithm. Depending upon the criteria's and constraints, cryptographic algorithm like Elliptic Curve Cryptography (ECC) is best suitable for WSN's environment. ECC has a smaller key size, high security and less computation time which makes the node an efficient crypto system. In order to protect the security of data, we propose a novel secure transmission strategy based on Cryptography. In this design, we acquire sensitive information securely so as to make use of the advantage of encryption. Our approach deal with the weakness of limitation in sensor node resources and the security threats, it is suitable for stream data in sensor nodes. The simulation experiments also demonstrate that this approach is effective in transmitting sensitive data covertly with the characteristics of lower energy consumptions and invisibility. This paper describes the implementation of ECC cryptosystem for WSN for secure key and data transmission between the nodes.

KEYWORDS: *WSN, IEEE 802.15, Cryptograhical, Remote Sensor*

How to cite this paper: Shahid Ishaq | Rashmi Raj "Analyzing & Securing Data Transmission in Wireless Sensor Networks through Cryptography Techniques" Published in International Journal of Trend in Scientific Research and Development (ijtsrd), ISSN: 2456-6470, Volume-4 | Issue-3, April 2020, pp.171-175, URL: www.ijtsrd.com/papers/ijtsrd30328.pdf

IJTSRD30328

INTRODUCTION

Wireless sensor network (WSN) is a self-organized multi-hop network composed of a large number of sensor nodes [1]. Each sensor node has the ability to sense data, process data, and communicates with others, so it is data-centric network. WSN is typically used in environment monitoring, healthcare, traffic management and battlefield. The data transmitted between the nodes may be sensitive (e.g. offensive weapon, troop movement, defense information). The whole network will be threatened if they are revealed by an eavesdropper. So it is vital for us to adopt effective strategy to ensure the transmission safety of the secret information.

In this paper, we propose a new secure transmission strategy based on encryption by using its characteristic which shrouds the data security without encryption, to aim at the weakness of limitation in sensor node resources and the security threats.

Unlike in existing schemes, it transmits data after embeds sensitive information into ordinary information. Compared with existing strategies, our strategy has obvious advantages. Transmitting the encryptive sensitive data can decrease the risk of communication from being monitored, intercepted and the communication overhead can be decreased. A real time hiding/extraction algorithm is proposed to stream data, which conceals and extracts the sensitive data effectively with low energy consumption.

The functionality of sensor nodes is limited by processing power, storage capacity, communication, and battery resources. The nodes are always exposed in open fields where they are unreachable. Any node may become a attack target with external and internal security risks including eavesdrop, DoS (Denial-of-Service), leak, tamper, infuse, playback, misguide, disrupt and others.

WSN needs to guarantee the security of network, nodes and data, while the security of the data is the most important including confidentiality, authentication, integrity and Freshness. The existing threats in WSN could be solved by making use of the data security technology to a great extent.

Cryptography and digital watermarking are the two major data security technologies. At present, the mechanism to solve this is mainly cryptography based such as data encryption, message authentication, integrity ensuring and broadcast validation. The available asymmetric cryptography and other ciphers cannot suitable due to the hardware restrictions. So researches of data security focus on key establishment, exchange, distribution and management mostly. Examples include pre-distribution, random key assignment, pair-wise key scheme, group-wise key scheme, and etc.

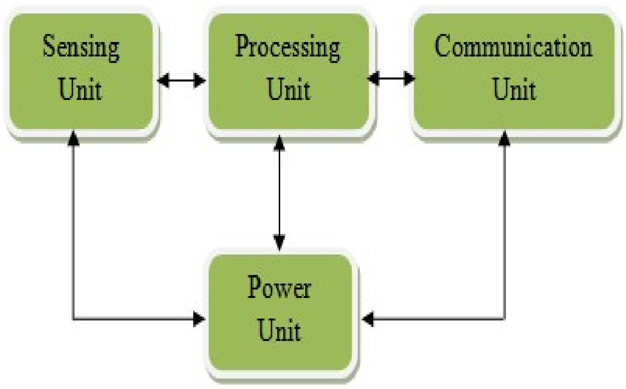


Fig No. 1.1: Basic blocks of Sensing Networks

The authentication and key management technologies in WSN become burdensome, which depend on the security of key heavily. It is difficult to be solved entirely only by secure key. Designing a new security mechanism, obviating potential security problem effectively and reducing security threat are hard assignment. New approaches are required for WSN development and application.

As the WSN's communication is open, WSNs are highly susceptible and at high risk, thereby effecting the entire system, if suitable safety measures are not taken. Authentication between WSN's plays an important role in securing data transmission against various types of attacks like node impersonation, falsification of data, replay attacks etc. Another issue is that WSN's are a combination of many tiny and low-cost sensor nodes where they have limited energy and limited computation ability to processor transmit the data. Thereby securing WSNs with it presents environmental resource-constrained has been becoming a challenging task. WSN's is a combination of multiple self organized sensor nodes capable of communicating wirelessly and security requirements are similar to any usual computer networks [1, 2]. As the WSNs have various constrains, all security solutions applicable for conventional computer networks

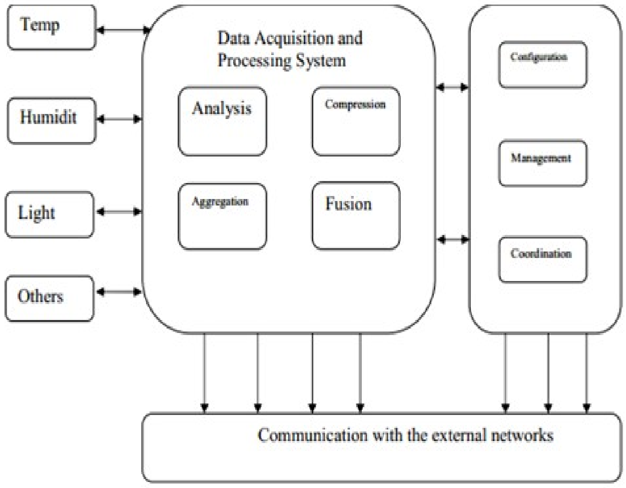


Fig No. 1.2: Functionality of a Sensor Node

Problems to be Evaluated:

Proposed a proficient gathering key exchange convention in view of a direct mystery sharing for remote sensor systems (WSNs), if aggregate key validation. Security examination for conceivable assaults is incorporated. Therefore, this convention can oppose potential assaults and furthermore fundamentally diminish the overhead of framework execution.

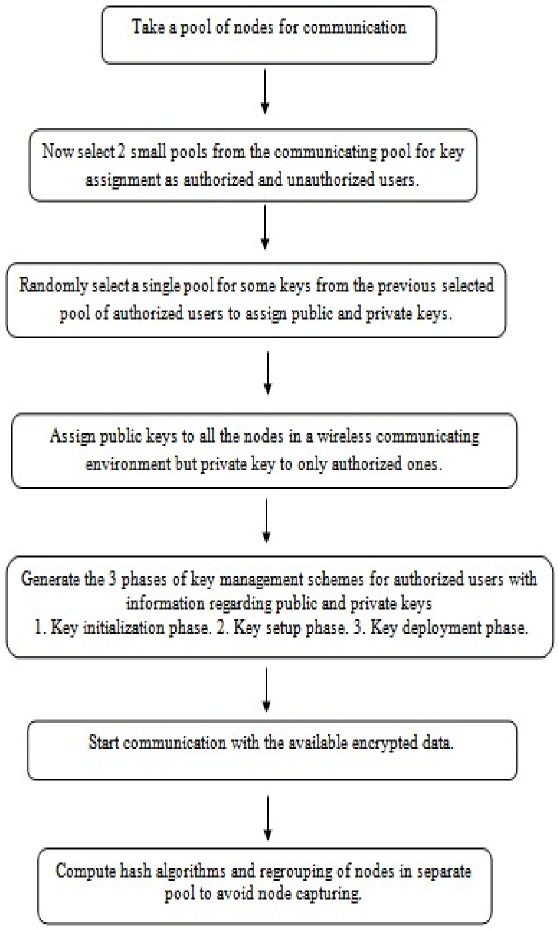
Proposed Algorithm:

Here we have implemented ECC for WSN on a Matlab simulator. From the survey made in our earlier stages, we can conclude that ECC is a better algorithm than RSA as it requires smaller key without compromising with the security aspects. We have tried to implement a topology.

One of the major concerns is the mutual authentication between the nodes in WSN's. This issue is resolved by the proposed ECC technique used for secure data communication.

In our topology there is a Sender and a Receiver, where they are communicating and data transfer takes place among them self. We also have shown an attacker as Eve, who also tries to access the data transmitted between the Sender and the Receiver. Since the data and WSN nodes, both are in open and vulnerable for attackers, there is a need for security within the nodes and for the data. By implementing ECC in WSN, the nodes can securely transmit data. The Sender and Receiver each generate their own Private Key and Public Key for each others. These keys are generated using the elliptic curve and the points on that curve generated. Both the Sender and receiver decide on to which curve and the finite points. When a node wants to communicate or send date with some other node, then the sender node uses its own Private Key and the Public Key of the intended node to generate a Shared Key. This Shared Key is used for Encryption of the data to send across other nodes. Once a node receives a data, the receiver also generates a Shared Key. This Shared Key is used for Decryption of the data at the receiver end. On the other hand the Eve also receives the Public Keys generated by both the Sender and the Receiver nodes. We also try to show that the Eve in spite of having the Public Keys of both the nodes still cannot generate the Shared Keys as the Eve does not have the Private Keys of both the nodes, thus securing the data. We also show that even if the Eve generates same set of points in the elliptic curve and assuming that Eve also has same set of finite points, still it is not possible for the Eve to generate the Shared key. By the time Eve tries to decrypt the data using various keys, next set of data transmissions are over

.


Take a pool of nodes for communication
Now select 2 small pools from the communicating pool for key assignment as authorized and unauthorized users.
Randomly select a single pool for some keys from the previous selected pool of authorized users to assign public and private keys.
Assign public keys to all the nodes in a wireless communicating environment but private key to only authorized ones.
Generate the 3 phases of key management schemes for authorized users with information regarding public and private keys
1. Key initialization phase. 2. Key setup phase. 3. Key deployment phase.
Start communication with the available encrypted data.
Compute hash algorithms and regrouping of nodes in separate pool to avoid node capturing.

Results:

In the wake of performing nuts and bolts of calculation we have gotten taking after reproduction comes about indicating essentials of encryption unscrambling comes about. Utilization of this symmetric calculation gives us the outcomes demonstrating that the this calculation is more suited over the uneven ones as the symmetrical calculations are more dependable with variable key administration era procedures giving productive security objectives as the key size is in distinguishable and shifted at each progression without being in need to make them known to all hubs in a system as private key is not figured by open key of the system gave as a security highlight of deviated cryptosystems. Likewise the symmetrical cryptosystems are more effective in security objectives accomplishment when contrasted with asymmetrical ones as they have to give the connection keys publically which causes unapproved assaults and client's information security surrenders.

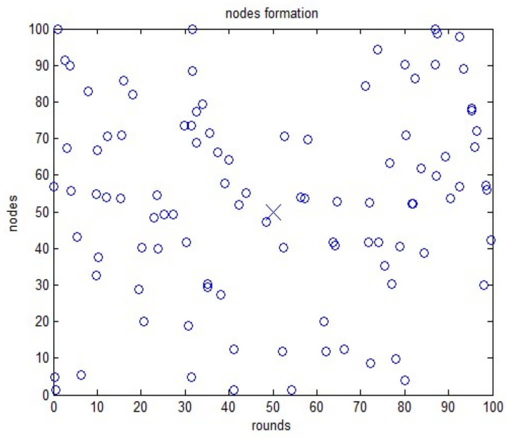


Fig No. 1.3: Nodes formation for base paper.

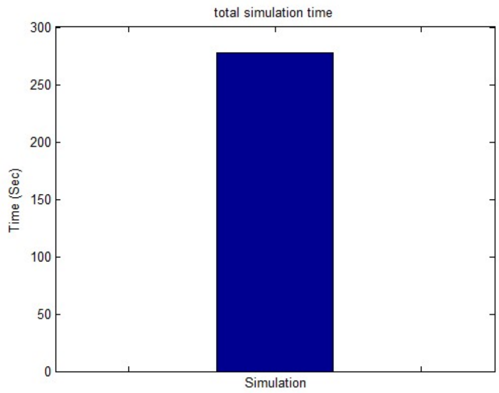


Fig No.1.4: Total stimulation time graph

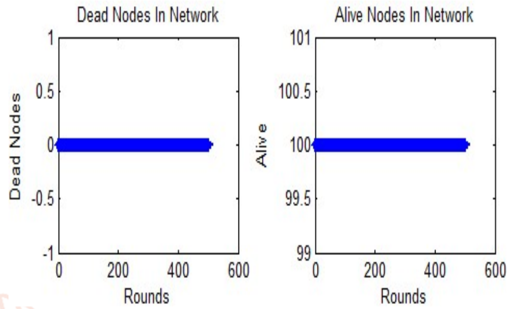


Fig No 1.5: Simulation time required and dead and alive nodes information of base paper

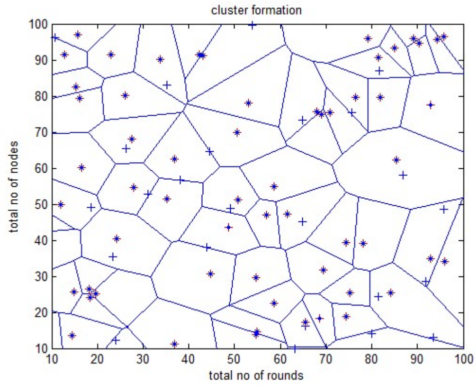


Fig No 1.6: Simulation cluster formation

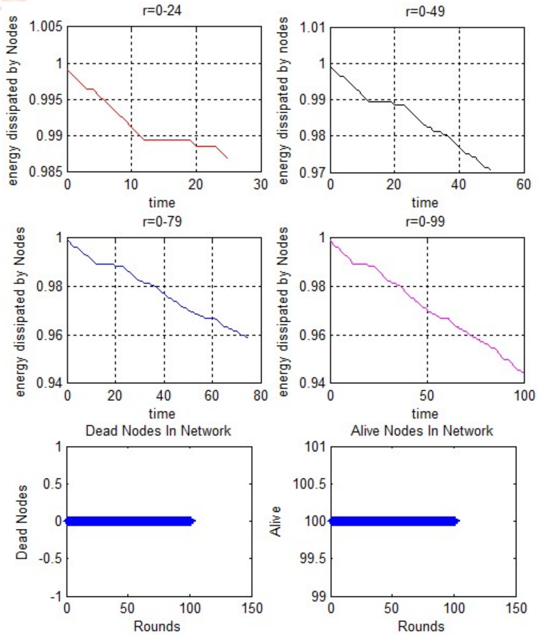


Fig No 1.7: Energy dissipation over time of proposed work simulation results

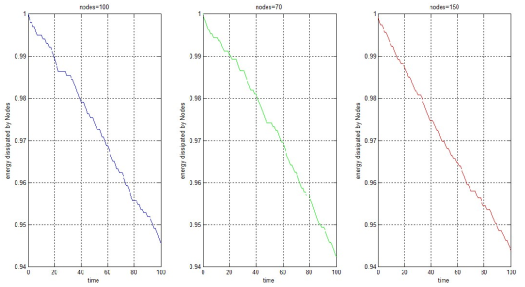
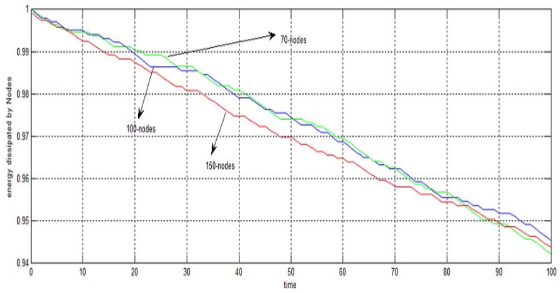
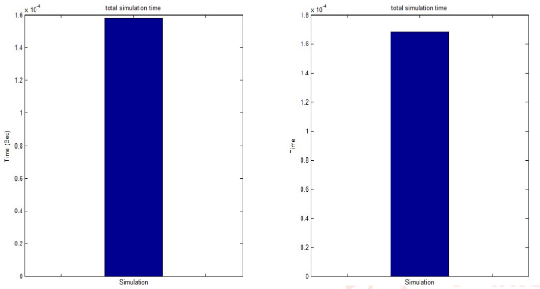


Fig No 1.8: Comparison of nodes-70,100,150 for energy dissipation graphs for proposed work.





a) For base work-total stimulation time b) for proposed work-total stimulation time

Fig No 1.9: Nodes comparison for energy dissipation graphs for proposed work

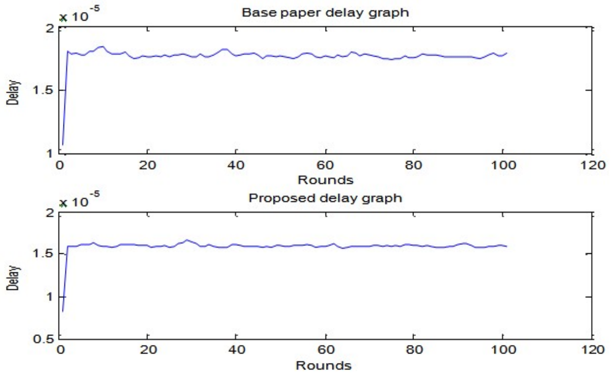


Fig No 1.10 : Delay graphs of 100-nodes-comparision b/w base paper and proposed work

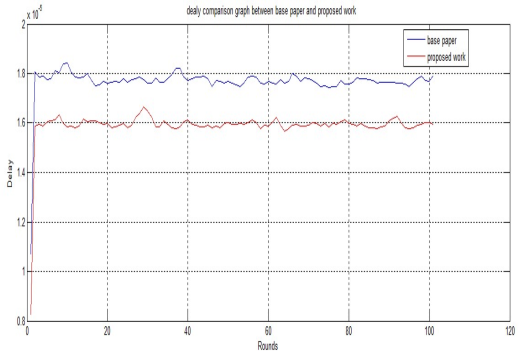


Fig No 1.11: Combined delay graphs between base paper and proposed work

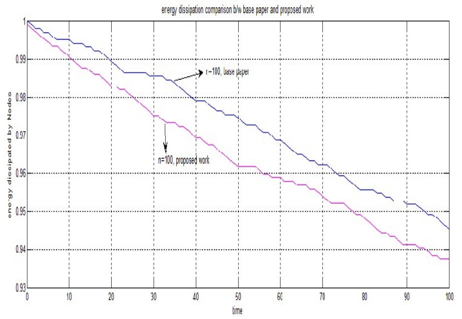


Fig No 1.12 : Comparison graphs between base paper and proposed work on the basis of energy dissipation

Conclusion:

We have compared files of various sizes and compared both the algorithms. The results are also shown in terms of bar graphs as shown. The comparison has been made with the standard algorithm, which is a traditional and the most used algorithm, with proposed algorithm. In our findings, here it is clearly seen that ECC consumes more time once in the beginning, we can see that, for a file size of 7 KB the encryption is drastically more for encryption and from 12 KB it requires less time and increases gradually for encryption. Though ECC requires more time for encryption, the key size is too small compared to RSA. However the decryption time taken by ECC is very less than the traditional RSA algorithm, even if the file size increases as shown. The decryption time for ECC is nearly similar for all files compared to RSA algorithm. Compared with the other three results, our obtained results are better by an average of 20%. The implementation of Elliptic curve can be further extended to implement on hyper elliptic curves on WSN. Further the ECC can also have various types of point generation methods on the curve and ECC can also be integrated with other cryptographic algorithms for additional security.

ACKNOWLEDGEMENT

I express my sincere gratitude to the I.K.Gujral Punjab Technical University, Jalandhar for giving me the opportunity to work on the thesis during my final year of M.Tech. I owe my sincerest gratitude towards Dr. Prabhjot Kaur, Director Engg, Universal Institute of Engineering and Technology, Lalru, for valuable advice and healthy criticism throughout my thesis which helped me immensely to complete my work successfully.

I would like to express a deep sense of gratitude and thanks profusely to Er. Rashmi Raj Assistant Professor, Department of Electronics & Communication Engineering, UIET, who was the thesis Supervisor. Without the wise counsel and able guidance, it would have been impossible to complete the thesis in this manner.

I would like to thank the members of the Departmental Research Committee for their valuable suggestions and healthy criticism during my presentation of the work. I express gratitude to other faculty members of Electronics & Communication Engineering Department, UIET, for their intellectual support throughout the course of this work.

References:

[1] T. Gao, D. Greenspan, M. Welsh, R. R. Juang, and A. Alm, "Fundamental signs observing and understanding following over a remote system," in Proc. IEEE 27th Annu. Int. Conf. Eng. Med. Biol. Soc. (IEEE-EMBS), Jan. 2006, pp. 102–105.

[2] L. Gu et al., "Lightweight recognition and grouping for remote sensor arranges in reasonable conditions," in Proc. third ACM Conf. Implanted Network Sensor System, Nov. 2005, pp. 205–217.

[3] G. J. Pottie and W. J. Kaiser, "Remote incorporated system sensors," Communication ACM,vol. 43, no. 5, pp. 51–58, 2000.

[4] L. Eschenauer and V. D. Gligor, "A key-administration plot for dispersed sensor systems," inProc. ninth ACM Conf. CCS, 2002, pp. 41–47.

[5] H. Chan, A. Perrig, and D. Melody, "Irregular key pre appropriation plans for sensor systems,"in Proc. IEEE Symp. SP, May 2003, pp. 197–213.

[6] W. Du, J. Deng, Y. S. Han, S. Chen, and P. K. Varshney, "A key administration conspire forremote sensor systems utilizing organization learning," in Proc. IEEE INFOCOM, Mar. 2004, pp.586–597.

[7] A. Rasheed and R. Mahapatra, "Key redistribution plans for building up pairwise keys with aversatile sink in sensor systems," IEEE Trans. Parallel Distrib. Syst., vol. 22, no. 1, pp. 176–184,Jan. 2011.

[8] S, Ruj, A, Nayak, and I. Stojmenovic, "Pairwise and triple key dispersion in remote sensor systems with applications," IEEE Trans. Comput., vol. 62, no. 11, pp. 2224–2237, Nov. 2013.

[9] F. Li and P. Xiong, "Reasonable secure correspondence for incorporating remote sensor systems into the Internet of Things," IEEE Sensors J., vol. 13, no. 10, pp. 3677–3684, Oct. 2013.

[10] R. Blom, "Non-open key appropriation," in Advances in Cryptology, D. Chaum, R. L. Rivest, and A. T. Sherman, Eds. New York, NY, USA: Plenum, 1982, pp. 231–236.

[11] Daehee Kim, Sunshin —Efficient and Scalable Public Key Infrastructure for Wireless Sensor Networks||, This work was partly supported by the National Research Foundation of Korea (NRF) grant funded by the Korea government (MEST), (No. 2012KlA3AlA09026959) 978-1-4799-5874-0/14/©2016 IEEE.