Energy Consumption in Key Management Operations in WSNs

Ramandeep Singh[1], Amandeep Kaur Virk[2]

[1]M.Tech Research Scholar, Department of Computer Science Engineering,
Sri Guru Granth Sahib World University, Fatehgarh Sahib, India

[2]Assistant Professor, Department of Computer Science Engineering,
Sri Guru Granth Sahib World University, Fatehgarh Sahib, India

Abstract: ***This paper gives an illustration and demonstration of mathematical model of new key management scheme which overcomes the limitation of Pre-Shared key scheme in terms of energy consumption using various key management operations in WSNs. Various key management operations were recorded and evaluate based on energy consumption at each step of authentication in wireless sensor network which improves that NchooseK Scheme is more scalable and secure than PSK in terms of energy consumption in WSNs.***

Keywords: Wireless Sensor Network, Key Management Operations, Pre-shared Key (PSK), NchooseK Algorithm**.**

1. Introduction

Wireless Sensor networks usually consist of a large number of ultra-small autonomous devices. Each device, called a sensor node, is battery powered and equipped with integrated sensors, data processing, and short-range radio communication capabilities [1].These sensor networks pose security and privacy challenges when deployed in a hostile environment. For example, an adversary can easily gain access to mission critical or private information by eavesdropping on wireless communications among sensor nodes. Therefore, security services are important to encrypt the wireless communication, for preserving the confidentiality, integrity, and availability of the transmitted data [2].

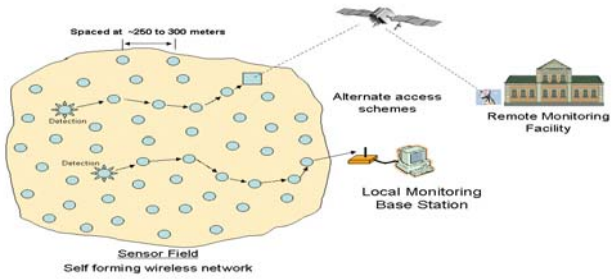

Figure 1: Working of WSN [3].

Key Management is the most important issue in the security of Wireless Sensor Networks. It helps in maintaining the confidentiality of secret information from unauthorized users. Sometimes, it is also useful for verifying the integrity of exchanged messages and authenticity of the sender. Keys are fixed length streams of random bits, which are known to only the authorized parties. Sender encrypts data / information in the key i.e. performs mathematical operations on data / information and key collectively. This produces a stream of bits, which does not reveal any information about the original stream of bits. Only authorized parties can decrypt or come to know original data / information [4].

2. Related Work on Key Management Schemes

Gaurav Jolly et al [5] have concentrated on the key management aspect of the security functionality using a Low-Energy Key management Protocol. Key management is essential for any cryptographic security system. They present an energy-aware approach for managing the cryptographic keys in a clustered sensor network. Shared symmetric keys are pre-deployed into the sensors and gateways (the cluster heads), requiring each sensor node to store only two secret keys. Separate protocols handle network bootstrapping, sensor addition/revocation, and key renewals.

Sai Ji et al [6] have proposed a novel key management scheme for the dynamic WSNs. In their paper the security authentication and random key distribution were initialized in the network deployment phase. During the network stable phase, in order to ensure the real-time update security for the network topology, their scheme proposed a dynamic updated key based on the AVL tree. At the end, the Simulation results show that their program can ensure the WSN's dynamic security as well as achieve the energy efficiency goal.

Madhuri Prashar et al. [7] have proposed in this paper about the overview and implementation of Pre-shared key Scheme (PSK) in WSN and based on the results of its implementation, limitations of PSK scheme are shown in terms of connectivity and energy efficiency. To overcome limitations of pre-shared key scheme, they compare it with Binomial Pyramidal Algorithm for key management, which improves the key connectivity of WSN and make it more energy efficient. In Binomial Algorithm, the privacy of keys is between server and client. In this scheme the key distribution is at run time. The memory required for the entire simulation is less as compare to PSK. The rate of drop packets is comparatively low to PSK. There is low consumption of energy using Binomial Algorithm.

Biswajit Panja et al [8] have described a group key management protocol for hierarchical sensor networks where instead of using pre-deployed keys, each sensor node generates a partial key dynamically using a function. The function takes partial keys of its children as arguments. The design of their protocol is motivated by the fact that traditional cryptographic techniques are impractical in sensor networks because of associated high energy and computational overheads. The group key management protocol supports the establishment of two types of group keys; one for the nodes within a group (intra-cluster), and the other among a group of cluster head (inter-cluster). Their protocol handles freshness of the group key dynamically, and eliminates the involvement of a trusted third party (TTP). They have experimentally analyzed the time and energy consumption in broadcasting partial keys and the group key under two sensor routing protocols (Tiny-AODV and Tiny-Diffusion) by varying the number of nodes and key sizes. The performance study provides the optimum number of partial keys needed for computing the group key to balance the key size for security requirements and the power consumption. The experimental study also concludes that the energy consumption of SPIN increases rapidly as the number of group members increases in comparison to our protocol.

3. Proposed work

The previous study on key management schemes is related to the packets delivered and received from one sensor node to another. The previous study on key management schemes does not mention how much energy a sensor node consumes while sending or receiving the packets from one node to another. The energy consumption in key management schemes in WSNs is an important issue. The proposed work is based on the analysis of energy consumption patterns in key management schemes (PSK/NchooseK) [9]. Different schemes will have different energy consumption patterns due to its complexity, level of access and security parameters. Here, we propose a comparative model based on the limitations and disadvantages of such key management schemes and compare the key management schemes related to energy consumption pattern and find out which scheme is better and consumes less energy while sending and receiving the data from one node to another in WSNs.

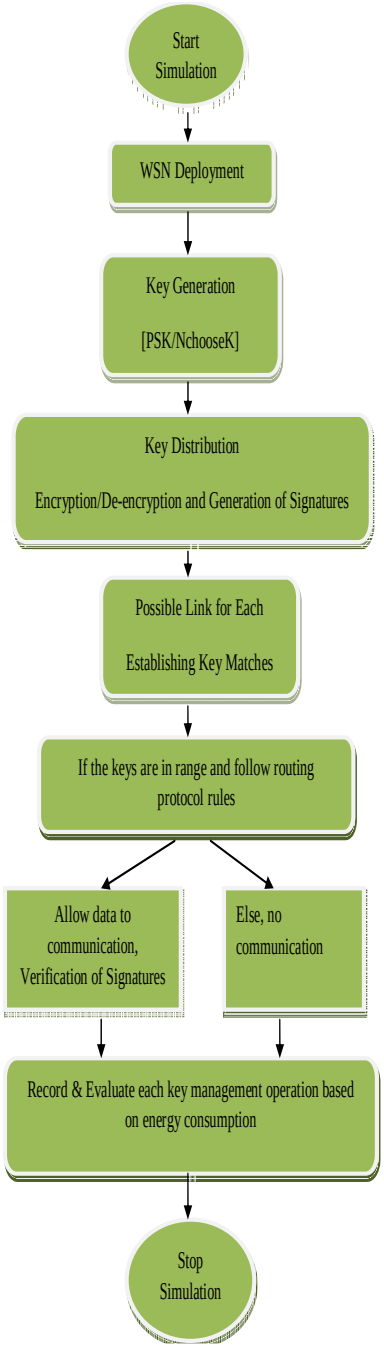

Figure 2: Simulation Overview

Once the simulation starts, the sensors are deployed in the network. The network is then bifurcated into server sensors and the client sensors. Then the keys are generated using NchooseK and PSK. The keys are generated to each sensor node. The keys are distributed among sensor nodes in the network .After distributing the keys the RSA cryptography is used to provide the secure communication among the sensor nodes for sending and receiving the data or information. In this step each sensor node have a public and a private key , the sensor node sends the data by encrypt the data and generating the signature in a cipher text . After that, another sensor node de-encrypts the data or information sent by first node by using a private key. Then the link is established if the second node matches with the key of first one. After matching process if the keys are in range and follow a routing protocol rules then the communication between sensor nodes establish otherwise there is no communication

link occurs .If the communication occurs then record and evaluate key management operations based on energy consumption and the simulation stops.

It is apparent from the dataset generate for result analysis that as there is disclosure of secrecy of key in the PSK scheme, so there is occurrence of fluctuation of energy pattern for different distinct of time. In other words, due to some limitation of PSK scheme the rate of energy pattern may varies for different interval of time which is shown in the graph below. The below graphs does not clearly demonstrate the energy pattern which is somehow limitation for PSK (Pre Shared / Pre loaded) Key distribution. It is apparent from the below results, that there is steady increase of energy with a distinct pattern with passage of time by applying NchooseK key Distribution Scheme. So, the data set seems to have steady values that depict the energy readings in the WSN, which constitutes the energy components in the simulation or in the whole process is recording increases in energy cost as the network increases in size. As there is fluctuation of energy in the data of PSK (Pre-shared / Pre-loaded) as whole were of not much help in calculating all the operation in one go, we have used the energy readings in such a manner that it depicts for each key operation [Generation, Verifications, Initialization etc].

4. Experimental Results for Each Key Management Operations Based on Energy Consumption

4.1 Initialization of Keys

In case of PSK scheme of Key Management the Keys are initialized once when the Wireless sensor network is deployed and when they are in process of reset or redeployment or in case reallocation of co-ordinates due to movement or ad-hoc nature the wireless sensor network, therefore , it is it cost increases whenever , there is reset and same in case of NchooseK, the keys are renewed once the lease is complete, and generation and initialization once is required when it comes part of wireless sensor network . The reading recorded for energy consumption for NchooseK are shown below in the graph and it shows that it increases as the network size increases and it has to generate more n number of keys pairs to be used as private and public keys , its energy consumption is directly proposal to the number of duty cycle or the frequency of key refreshment , However , the initialization of Keys in case of the NchooseK is slightly more as the generation and distribution has to calculate factorial however initialization operations are integrated and occur in one go. The following graph depicts the Energy consumption in operation of Encryption of keys. The encryption of keys is done to provide the secure network between sensor nodes. The RSA cryptography is used to assign the public and private keys to each sensor node while sending and receiving the packets in a secure network. Because of pre-loading of the keys in PSK the encryption process is done already when the keys are generated. Due to pre-load of keys at the starting or when the keys are generated the encryption operation in PSK scheme requires less energy consumption as compared to NchooseK scheme.

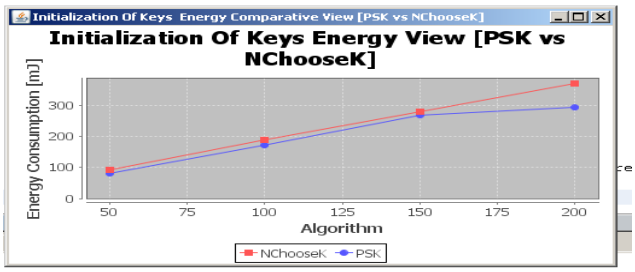

Figure 3: Comparative view of Initialization of keys

4.2 Generation of Keys

In case of PSK scheme of Key Management the Keys are made when the Wireless sensor are in process of being manufactured, therefore, it is one time cost and is assumed to be rationalized in calculations while doing comparative with the NchooseK key management with cost value of 0.1, in case of PSK, the keys are never generate once it is shipped and deployed as part of WSN. The reading recorded for energy consumption for NchooseK are shown below in the graph and it shows that it steadily increases as the network size increases and it has to generate more 'n' number of key pairs to be used as private and public keys, its energy consumption is directly proposal to the number of duty cycle or the frequency of key refreshment.

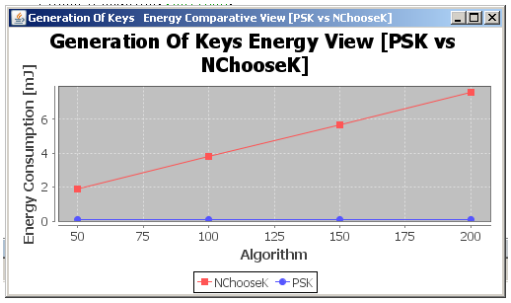

Figure 4: Comparative View of Key Generation.

4.3 Encryption, Generation of Signature and De-encryption of Keys

The encryption of Keys in both cases is different in-spite of the fact both are using same RSA algorithm for encryption and de-encryption, this may be attributed to fact and PSK creates more network voids as compared to NchooseK scheme as it generate such keys that can more successful combinations of key match, hence the NchooseK key management scheme consumes a little less energy in exchange (communication).

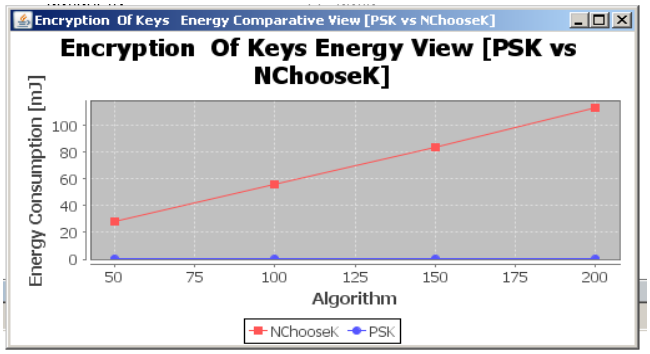

Figure 5: Encryption of keys energy comparative View.

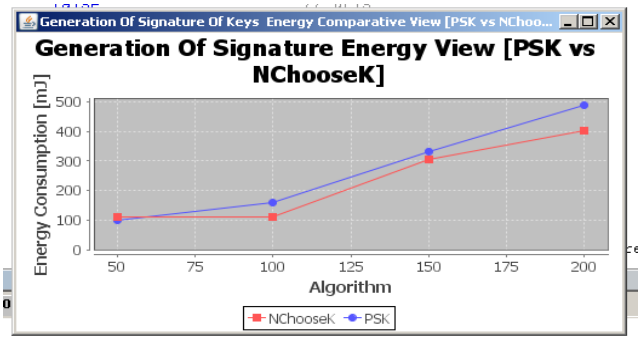

Figure 6: Generation of signature energy comparitive view.

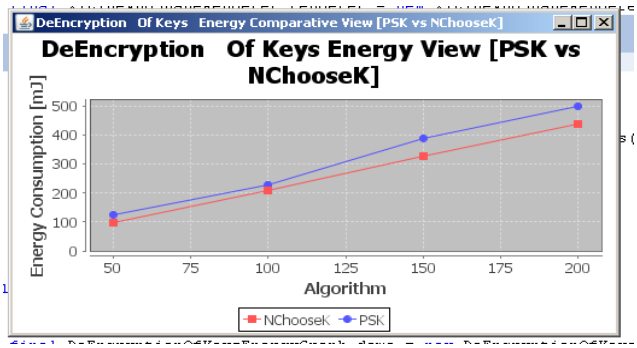

Figure 7: De-encryption of keys Energy Comparative View.

4.4 Verification of Signature

The following Graph depicts the Verification of Signature after the de-encryption of keys. The verification of signature is done when the each node in the network matches with the node having same key code. For exp: each sensor node in the network is assigned by different keys when the sensor node matches with the same key node the communication starts otherwise not. In the verification of signature operation, when the network size is 50, the NchooseK scheme consumes less energy as compared to the PSK. At the highest network size of 200 nodes, the NchooseK consumes again the less energy than PSK.

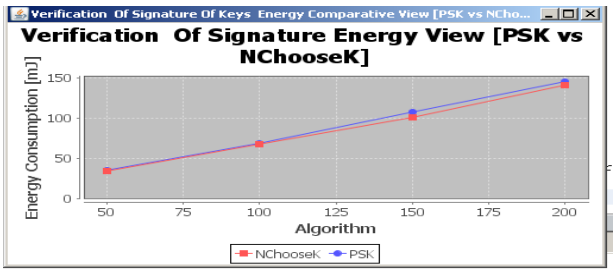

Figure 8: Verification of signature energy comparative view.

4.5 Communication of keys

In case of PSK scheme of Key Management the Keys are generates and encrypted once (by manufacturer of the wireless sensors) and the initialization is also done once when the Wireless sensor network is deployed and when they are in process of reset or redeployment or in case reallocation of co-ordinates due to movement or ad-hoc nature the wireless sensor network, therefore , it is it cost increases whenever , there is reset and same in case of NchooseK, the keys are renewed once the lease is complete, and generation, encryption and initialization of the key is done when it comes part of wireless sensor network .During all these steps the communication step is established. Due to which the exchange of information from one sensor node to another is done and this depicts that how much energy is consumed while sending and receiving the information from one node to another by comparing the PSK scheme and NchooseK scheme and the results show that the NchooseK scheme is better than PSK because of consuming less energy as compared to PSK shown in figure.

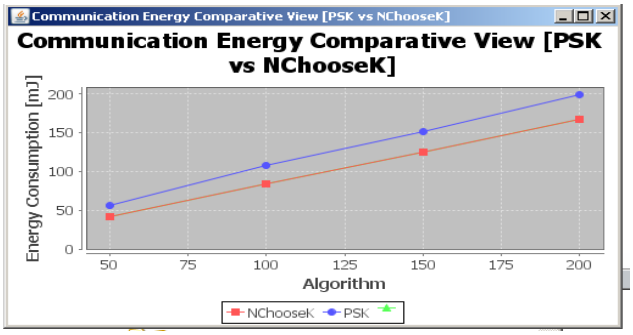

Figure 9: Communication energy comparative view

5. Conclusion

Reducing the number of key negotiation process is real way to reduce the consumption of the energy in wireless sensor networks and similar inference can be concluded in case of memory. In case PSK, the initialization and generation of key would always be less, if it is compared to the some dynamic key generation and initialization key management protocol like N choose K [9], this is attributed to the fact when every time it the lease of the key comes to end due to end of duty cycle it need to do these two operations again. However, it is known and proven fact in case of PSK, security and scalability reduces its efficiency when deployed in wireless sensor networks.

Since, vast quantities of sensor nodes are distributed in the network, extremely low cost and low power become the core design challenges. The low cost constrains the resources that can be implemented on the devices, and low power requires the operations to be done in a highly efficient way and this is possible only if without comprising the security we are able to reduce the failed connections that might occur when key negotiation fails to large disjoint sets of private and public key leading to network void , this is reduced in case of N choose K key management scheme , that is why the other operations like verification of signature is taking less energy as compared to the PSK scheme of key management.

6. Future Scope

The Key management will remained a challenging issue in wireless sensor networks (WSNs) due to the constraints of sensor node resources. Various key management schemes that trade-off security and operational requirements have been proposed in recent years including our research work on finding which key management schemes consumes how much energy at which kind of operation, therefore, for future scope we suggest that by first by examining the security and operational requirements of WSNs and then after, further

reviewing more key management protocols like Eschenauer, Du, LEAP, SHELL, and Panja. Eschenauer's scheme which is classical random key distribution schemes for WSNs. We must come out with new algorithm that can improve on Random Key management by using key matrices not only this which key management scheme provides a highly flexible key management scheme .Different types of keys like SHELL, which focuses on achieving high robustness, and Panja is optimized for hierarchical WSNs. LEAP, SHELL, For eg: Panja support cluster-based operations and are more aligned with current trends as shown by the new standards, IEEE 802.15.4b and the ZigBee "enhanced" standard can be explored and improved. Future developments likely can incorporate the features of different key management schemes and adjustable robustness enhancements from scalability point of view and must be extremely security-critical applications may benefit from restructuring the whole key negotiation process to ease implementation and maintenance.

References

[1] Soundarya.P and Varalakshmi .L.M "Security in wireless sensor networks using key management schemes", International Journal of Computer Science & Information Technology (IJCSIT), Vol 2, No 6, December 2010.

[2] S. Saranya Devi, N.Suganthi "An efficient key pre-distribution scheme for wireless sensor network" International Journal of Communications and Engineering Volume 06– No.6, Issue: 04 March 2012.

[3] "Wireless Sensor Networks" www.days.nateg.org [Online].Available: http://days.nateg.org/2012/images/sessions/Wireless-Sensor-Networks.gif.html.[Accessed: NATEG © 2011 – 2013].

[4] Syed Muhammad Khaliq-ur-Rahman Raazi1, Zeeshan Pervez and Sungyoung Lee "Key Management Schemes of Wireless Sensor Networks: A Survey", Security of Self-Organizing Networks:MANET,WSN,WMN,VANET,Auerbach Publications,CRC press,Taylor&Francis Group USA,2009.

[5] Gaurav Jolly, Mustafa C. Kuşçu, Pallavi Kokate, and Mohamed Younis," A Low-Energy Key Management Protocol for Wireless Sensor Networks," IEEE Symposium on Computers and Communications (ISCC'2003).

[6] Sai Ji, Liping Huang and Jin Wang "A Novel Key Management Scheme Supporting Network Dynamic Update in Wireless Sensor Network", International Journal of Grid and Distributed Computing Vol. 6, No. 1, February, 2013.

[7] Madhuri Prashar and Rajeev Vashisht," Optimizing Pre-Shared Key Scheme For Effective Key Connectivity And Energy Efficiency In WSN", International Journal for Science and Emerging Technologies with Latest Trends 7(1): 1-10 (2013).

[8] Panja, Biswajit , Madria, S.K. , Bhargava, B. " Energy and communication efficient group key management protocol for hierarchical sensor NETWORKS", Sensor Networks, Ubiquitous, and Trustworthy Computing, 2006. IEEE International Conference (Volume: 1).

[9] Harjot Bawa, Parminder Singh and Rakesh Kumar "An Efficient Novel Key management scheme using NchooseK algorithm for Wireless Sensor Networks", International Journal of Computer Networks & Communications (IJCNC) Vol.4, No.6, November 2012.