International Journal of Modern Engineering Research (IJMER)
www.ijmer.com Vol. 3, Issue. 5, Sep - Oct. 2013 pp-2908-2915 ISSN: 2249-6645

A Security Framework for Replication Attacks in Wireless Sensor Networks

T. Subramani[1], S.Ravi Varma[2], R.Kabileshwaran [3]
[1]*Professor & Dean, Department of Civil Engineering, VMKV Engg College, Vinayaka Missions University, Salem, India*
[2]*Application Engineer, IBM Pvt. Ltd., India*
[3] *Application Engineer, IBM Pvt. Ltd., India*

ABSTRACT: *Mobile sinks play a great role in many Wireless Sensor Network applications for efficient data accumulation, localized sensor reprogramming and for collecting data from various sensor nodes across the globe. However, in sensor networks that make use of the existing three tier security framework, elevates a new security challenge i.e an attacker can easily create a replicated node and can gain control of the data in the network. Although the three-tier security framework is more resilient to mobile sink replication attacks, it is weak against access point replication attacks. To reduce the damage caused by access node replication attack, strengthening the authentication mechanism between the sensors and access nodes is vital. For this purpose, the single polynomial pool is converted to a double polynomial pool for providing security over the existing system. Also, security is increased by separating the access points into two layers namely, access nodes-D and access nodes-I along with a more secure authentication mechanism called WHIRLPOOL that produces a 512 bit encrypted text using Miyaguchi-Preneel scheme of cipher text generation.Our proposed algorithm ensures the necessary security mechanism for Wireless Sensor Networks and also does not degrade the performance of quality of service.*

Keywords: *Security, Replication Attack, Wireless Sensor Networks, Whirlpool, Key Management*

I. INTRODUCTION

A Wireless sensor network (WSN) consists of spatially distributed autonomous sensors. These sensors are used to monitor physical or environmental conditions, such as temperature, sound, pressure, etc. To cooperatively pass their data through the network to a main location, the more modern networks are bi-directional which enables control of sensor activity. The industrial and consumer applications, such as industrial process monitoring and control, machine health monitoring, and so on. Compromising security in networks is very easy unless we supply strong authentication schemes. The idea of using single polynomial pool is certainly outdated as it opens windows to many node replication attacks. Since single polynomial authentication is compromised, we move on to create two polynomial pools namely static polynomial pool and mobile polynomial pool. Static polynomial pool will supply keys to sensor nodes and access points whereas Mobile polynomial pool will supply keys to access points and mobile sinks [7].

Using two separate key pools and having few sensor nodes that carry keys from mobile key pool will make it more difficult for the attacker to launch a mobile sink replication attack on the sensor network by capturing only few arbitrary sensor networks. Although the above security approach makes the network more resistant to mobile sink replication attack compared to single pool based key pre-distribution scheme, it is still vulnerable to stationary node replication attack. In order to resist this attack, one-way hash algorithm is paired with static polynomial pool based scheme to enhance the security.

In order to enhance the security scheme, stationary nodes (access points) are divided into two layers Access Nodes-D and Access Nodes-I consisting of nodes with direct contact and nodes with indirect contact respectively.

1.2 KEY PRE-DISTRIBUTION

The term Key Pre-distribution could be defined as loading keys into sensor nodes prior to deployment. Two nodes find a common key between them after deployment. The various challenges in key pre-distribution are memory/energy efficiency, security and scalability.

II. RELATED WORK

2.1 SECURITY IN WIRELESS SENSOR NETWORKS

Many works in past has been carried out by various researchers. Some of the important citations has been presented here. Among them, Hasan Tahir presented his work on Wireless Sensor Networks. In his work, the current applications of wireless sensor networks are in the fields of medical care, battlefield monitoring, environment monitoring, surveillance and disaster prevention. Many of these applications require that the sensor network be deployed in an area that is hostile, inaccessible and mission critical. Keeping this in mind a network administrator has to see the security risks involved and how to tackle it if a security threat arises.

Security Methods for Wireless Sensor Networks is proposed by Xiuli Ren in which wireless sensor networks can be used for a wide range of potential applications such as military target tracking, environment monitoring, patient monitoring and scientific exploration in dangerous environments. When sensor networks are deployed in a hostile terrain, security becomes extremely important, as they are prone to different types of malicious attacks. Due to the resource limitations of sensor nodes, existing network security methods, including those developed for Mobile Ad-Hoc Networks, are not well suitable for wireless sensor networks.

Routing in Wireless Sensor Networks was proposed and implemented by Rachid Ennaji. Their system in which routing takes place using protocols such as AODV and DSDV. It brings out all methods to transfer data and also the best optimum protocol for each type of data transfer.

Stephen Olariu, et al presented his work Information Assurance in Wireless Sensor Networks, that assures security. However, a Wireless Sensor Network is only as good as the information it produces. But, the most important concern is information assurance. Information sent through wireless sensor nodes may be subjected to certain risks and danger. When considering very confidential data any flaw in security can be catastrophic.

Methods for Sensors Localization in Wireless Sensor Networks was discussed by Zenon Chaczko, et al. In their work, self-organization and routing algorithms dedicated to wireless sensor networks usually assume that sensors absolute positions are unknown and all decisions are based on sensors own local information. But sooner or later we need to find the positions of the sensor nodes for various purposes such as maintenance etc., so we need effective localization algorithms to find out the relative position of the sensor nodes.

Fatemeh Nourani, et al presented his work Improved Circles Intersection Algorithm for Localization in Wireless Sensor Networks in which they determined the relative position between nodes is very difficult. In fact it is an NP problem. Each node has its own range i.e., a circular range. Their paper brings out effective algorithms to find relative positions of nodes based on intersection of ranges. This idea is used by us in differentiating the direct and indirect contact nodes in the middle layer of the architecture.

An Efficient Approach for Sensor Deployments in Wireless Sensor Network was presented Sujata Dhanorkar that describes the connectivity can be defined as the ability of the sensor nodes to reach the data sink. If there is no available route from a sensor node to the data sink then the data collected by that node cannot be processed. Most of the works discuss in this paper deal with area coverage where the objective is to maximize the coverage percentage; ratio of area covered by at least one sensor to the total area of the region of interest (ROI). In addition, the relation between the number of sensors and efficient coverage area ratio is discussed.

2.2 KEY MANAGEMENT IN WIRELESS SENSOR NETWORKS

Similarly, many works have been proposed in the past and some of them are cited here. Eric Ke Wang, et al proposed an Efficient and Secure Key Establishment Scheme for Wireless Sensor Network. The data authentication becomes very important when transferring data. Key management and generation becomes a must to do task. But public key management is not secure enough. Their paper proposes an effective way to generate keys and enhance security using diffie-helmann key exchange algorithm.

A Key Management Method ofWireless Sensor Network was proposed by Xuemei You. In his work, the actual situation of current wireless sensor network pair-wise key management research, analysis and comparison between the existing two type of pair-wise key management solution is made according to the evaluation metrics proposed in this article. This cited paper brings out the fact that proper pair wise key management can be chosen according to the environment chosen. Also, this paper also brings out the basic limitations when we are using WSN.

Kirti Sharma, et al proposed Flexible and Efficient Scheme for Static Wireless Sensor Networks. Key distribution and management is the core issue of any security approaches. Due to extremely resource-constrained SNs and lack of any infrastructure support, traditional public key based key distribution and management mechanisms are commonly considered as too expensive to be employed in WSNs. Also, they have proposed an efficient individual, pair-wise and cluster key establishment mechanisms EIPCKM for static WSNs, which enable establishing secure links between any two SNs located within their communication range. It removes the Node Addition Attack, Node Cloning Attack and also increases the security within the cluster by introducing the cluster key.

The Study on Key Distribution and Management Mechanisms in Wireless Sensor Networks presented by Liu Feng states that the polynomial pools provide a wide range of good keys. In fact polynomial based key generation is widely used in most of the authentication mechanisms in WSNs.

Walid Bechkit, et al presented an Efficient and Highly Resilient Key Management Scheme for Wireless Sensor Networks. They used the concept of probabilistic key distribution. Deterministic schemes ensure that each node is able to establish a pair-wise key with its neighbors. To guarantee determinism, protocols such as LEAP make use of a common transitory key that is preloaded into all nodes prior to deployment.

Secure and Efficient Key Management Scheme for Wireless Sensor Networks proposed by Shobhit Tiwari that provides a key management technique to ensure maximum security of the wireless sensor network and also of every individual node subject to various hostile environments and situations. This scheme ensures that compromised sensor nodes are resilient towards attack before and after mutual pairwise path establishment. It is a self-enforcing scheme and analysis shows that it is more resilient to sensor capture attacks than the previous schemes.

Walid Bechkit, et al presented a New Key Management Schemes for Resource Constrained Wireless Sensor Networks.In their paper, without effective key management and generation the authenticity of the data sent moves to a questionable state. This paper brings out a concept called Hash chaining by which key pre-distribution schemes are established.

Research on Key Pre-distribution Scheme of Wireless Sensor Networks was presented by Zhao Jinchao, et al. A novel pairwise key management scheme to enhancing the security is proposed and part of keys in the key pool are computed by using hash function and the hash value are as new keys and put back into the key pool.

Vijay Anand presented the Dynamic Key Management Method for Wireless Sensor Networks that has a static key pool which gives us a greater risk of attack. They also proposed an idea of using dynamic generation of keys to reduce an attack. But this type of generation requires more computational time and a good processor with large processor speed.

Node Replication Attacks inWireless Sensor Networks was proposed byWen Tao Zhu in which replication attack makes it possible for an adversary to prepare her own low-cost sensor nodes and induce the network to accept them as legitimate ones. The adversary only needs to physically capture one node, reveal its secret credentials, replicate the node in large quantity, and deploy these malicious nodes back into the network so as to attack the network with little effort. Their paper brings to our attention the various attacks possible with WSNs and how to develop a contingency plan if an attack takes place.

2.3 CRYPTOGRAPHIC ALGORITHMS

There are many works pertaining to cryptographic algorithms. Some of the important works have been cited in the project work. Archana Tiwari, et al presented Performance Evaluation of Cryptographic Algorithms. They presented two most widely used symmetric encryption techniques Data Encryption Standard (DES) and Advanced Encryption Standard (AES). From their paper it is very much clear that DES and AES are very much fragile because of the avalanche effect.

Modied-DES Encryption Algorithm was proposed by Walid Zibideh, et al. In their work, due to the fact that wireless channels are an open medium to intruders and their attacks, encryption is a vital process to assure security over these channels. However, using well-known encryption algorithms to encrypt data in wireless communication will result in a catastrophic error due to the avalanche effect, which is implemented in these algorithms to assure security. In their paper, we propose a modication to the Data Encryption Standard (DES) to make it secure and prone to the bit errors caused by the wireless channel. We observe that using the modied algorithm in wireless channels, improves the Bit Error Rate (BER) performance as well as security compared to DES. But we have used the simple version of DES so that it can be used to efficiently simulate an attack. Based on the above literature survey, it is found that, still there is a need for further improvements over the existing work. Hence, we propose a new security framework for replication attacks in Wireless Sensor Networks that possibly tries to prevent such attacks in this project work.

III. WIRELESS SENSOR NETWORKS

A Wireless Sensor Networks is built of ”nodes” from a few to several hundreds or even thousands, where each node is connected to one (or sometimes several) sensors. Each such sensor network node has typically several parts: a radio transceiver with an internal antenna or connection to an external antenna, a micro controller, an electronic circuit for interfacing with the sensors and an energy source, usually a battery or an embedded form of energy harvesting. A sensor node might vary in size from that of a shoe box down to the size of a grain of dust, although functioning ”motes” of genuine microscopic dimensions have yet to be created. The cost of sensor nodes is similarly variable, ranging from a few to hundreds of dollars, depending on the complexity of the individual sensor nodes. Size and cost constraints on sensor nodes result in corresponding constraints on resources such as energy, memory, computational speed and communications bandwidth.

Security is important for many sensor network applications. Wireless sensor networks (WSN) are often deployed in hostile environments, where an adversary can physically capture some of the nodes. Once a node is captured, adversary collects all the credentials like keys and identity etc. The attacker can re program it and replicate the node in order to eaves drop the transmitted messages or compromise the functionality of the network. Identity theft leads to two types attack: clone and Sybil. In particularly a harmful attack against sensor networks where one or more node(s) illegitimately claims an identity as replicas is known as the Node Replication attack. The replication attack can be exceedingly injurious to many important functions of the sensor network such as routing, resource allocation, miss-behaviour detection, etc. This paper analyses the threat posed by the replication attack, several novel techniques to detect and defend against the replication attack, and analyses their effectiveness.

Wireless sensor networks are used in many applications, in sensing the environmental conditions and transmitting it over longer distances to the base stations. When the base station is far away from the sensing field (where sensors are fixed), the data is sent by a multi-hop. As the data is passing through multiple hops, an intruder can easily cause the attack at any stage in the network.

3.1 TOOL COMMAND LANGUAGE

Tcl is a Tool Command Language in which everything is represented as a string, although the internal interpretation may be of any kind. The command set is used for assingnment in tcl. In puts statement the argument must be preceeded with the $ sign , for procedures args can be passed as both values and names. E.g. Set a 10

3.2 NETWORK ANIMATOR

Network Animator(NAM) is a tool used for network simulation traces, supports topology layout and packet level animation. Provides integrated network monitoring within the switch. Collects the network traffic statistics for real time traffic analysis, performance monitoring and trouble shooting. NS with NAM is an efficient tool for dealing the networking concepts. All the routing protocols are in NS and these protocols can be very easily visualized with the NAM. NAM Graphical editor is a latest addition to the NAM, with this there is no need to create a tcl script separately to show the animation. We can make our own network topology, simulate the traffic sources.

3.3 NETWORK SIMULATOR

Network Simulator(NS) is a simulator used for research in networks. It supports for simulating Transmission Control Protocol(TCP), routing and multicast protocols over wired and wireless networks. Software used to predict the characteristics of large scale complex network systems. Discrete event simulator uses C++ with oTcl interpreter shell (user interface) which allows the i/p model files to get executed. Almost all network elements are developed as classes. It supports a class hierarchy in C++, very similar class hierarchy in oTcl. The root of this class hierarchy is Tcl Object. User tend to create a new simulation objects through the oTcl interpreter and these objects get mirrored by corresponding objects in the class hierarchy in C++.

3.4 SPECIFICATIONS OF WIRELESS SENSOR NETWORKS

3.4.1 Access Points

These are the intermediaries in data transfer. Some of the mobile sinks acts as intermediates. They share keys from both the key pools (static and mobile key pool). Keys from the static key pool facilitates the data transfer between the sensor nodes and them, while the keys from mobile key pool provides authentication for the data transfer between them and the mobile sinks.

3.4.2 Mobile Sinks

Mobile sinks informs the sensor nodes about their location updates, frequent changes in the locations of the mobile sinks causes the sensor nodes to collide in the network. Instead of transferring the information to the entire network at each time, the sinks broadcast the update to the local LAN

.

3.4.3 Key and Key Pools

In order to maintain security, it is very important to encrypt the messages sent among the nodes, so keys must be mutually agreed by the communicating nodes. Establishing the keys for the wireless nodes is a challenging task. Key agreement schemes such as Diffie-Hellman and public key schemes are not suitable for wireless sensor networks. Key pre distribution depends upon the size of the key pool, and the maximum size of the key pool that can be used by the scheme would be s2p, where s is the size of the key pool and p is the probability that two nodes share a common key. Key pre distribution is also not possible since it consumes large amount of memory when the network size is large. So instead of assigning key prior to the data transmission, a scheme is proposed to assign keys randomly [2].

IV. ENHANCED THREE TIER SYSTEM ARCHITECTURE

Basically a sensor node in a wireless sensor networks performs some operations, gathers information and communicates with the other nodes. The main components of the sensor nodes are micro-controller, transceiver, external memory and power source. The enhanced three tier architecture scheme discussed here consists of four layers namely sensor nodes, access nodes with direct contact, and access nodes in indirect contact and mobile sinks. At the initial stage keys from the single polynomial pool has been shared between the sensor nodes and the mobile sinks for communication. Since the single polynomial has been used, the attacker can easily replicate the node, capture the key and misbehave in the network. Therefore in order to enhance the security, two polynomial pools namely static polynomial pool and mobile polynomial pool are created which is called the three tier security mechanism. Even though there is a security mechanism by sharing key from two polynomial key pool for layered communication between layers, the replication attacks still persists.

The attacks that are possible in the three tier security scheme are mobile sink replication attack and access point replication attack, out of which mobile sink replication attack is reduced to small percentage by the implementation of this scheme. In order to avoid the access point replication attack, it is divided into access points which are in direct contact with the sensor nodes mobile sinks and access points which are not in direct contact with the sensor nodes-mobile sinks. In this enhanced scheme, keys from static polynomial pool is shared by the following layers namely sensor nodes, D access nodes, I access nodes. And keys from the mobile polynomial pool are shared by the following layers namely I access nodes and mobile sinks. The access nodes which are in indirect contact share the keys from the mobile polynomial pool and some percentile of keys from the static polynomial pool. Therefore an attacker who captures an access node will get either a static key alone or both static and mobile key(hybrid key).

By capturing a node with the direct contact, which has only static key, an attacker cannot be able to send the data to intended destination because the data will be re routed. Once again an attacker capturing the access node which is indirect will get both the keys, but then also it is least possible for an attacker to reach the destination as intended. The following architecture describes the enhancement of the three tier security scheme, which is more resilient towards replication attacks [3].

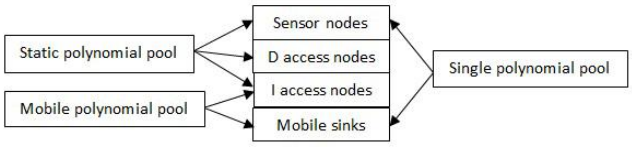

Figure 4.1 Enhanced three tier Architecture

4.1 LAYER CONSTRUCTION

In wireless sensor networks, to implement the enhanced scheme stated above three layers are to be created namely sensor nodes, access nodes and mobile sinks. Transmission control Protocol is used in communication to transfer the data between the layers. A single polynomial pool is created. Keys from this pool are used for communication between sensor nodes- access points and access points-mobile sinks. The figure 4.2 depicts the same.

4.2 KEY POOL SEGREGATION

To enhance the security scheme, two polynomial key pools are created. Keys from static polynomial pool are used for data transfer between sensor nodes and

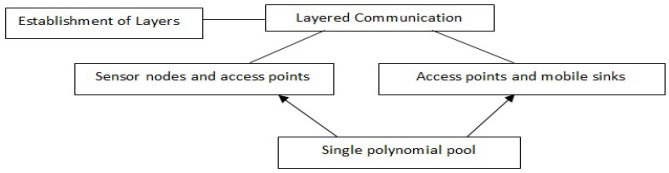

Figure 4.2 Layer Construction

access points and a key from the mobile polynomial pool is used for data transfer between access points and mobile sinks., which is described through the below block diagram in figure 4.3.

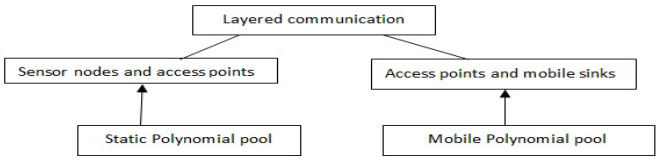

Figure 4.3 Key Pool Segregation

4.3 SECURITY ENHANCEMENT

The access point layer is separated into nodes with direct and indirect contact with respect to interference range. An enhancement of Advanced Encryption standard called the Whirlpool algorithm is used for authentication between access points and the mobile sinks. Once the layer is segregated and key distribution is done coupled with strengthening by means of Whirlpool algorithm, the probability of the attack decreases, i.e. an attacker cannot easily create a replicated node, and transfer the data. The following block diagram describes the steps to be carried out after implementing the three tier security approach.

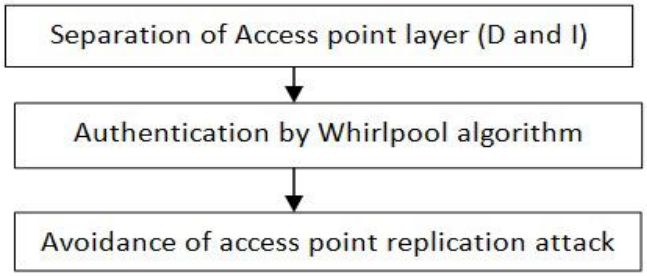

Figure 4.4 Security Enhancement

V. SECURITY MECHANISMS

5.1 DATA ENCRYPTION STANDARD

DES is a 64-bit block cipher. Both the plain text and cipher text are 64 bits wide. The key is 64-bits wide, but every eighth bit is a parity bit yielding a 54-bit key. The DES algorithm involves a step by step procedure or rounds to make up the cipher text needed. The initialization round is where the plain text is subjected to initial permutation and is split into left and right sub parts [6] [4].

Before the start of the first round the key that should be used is subjected to various processes. The 64 bit key is converted into a 48 bit key. After the key is prepared the execution of rounds start.The left and the right part of the plain text is permuted,XORED and then the output this round is given as input to the next round. The number of rounds depend on the length of the plain text. This algorithm is no longer in use because it can be easily attacked. So simulating an attack becomes easier if we use the above algorithm.

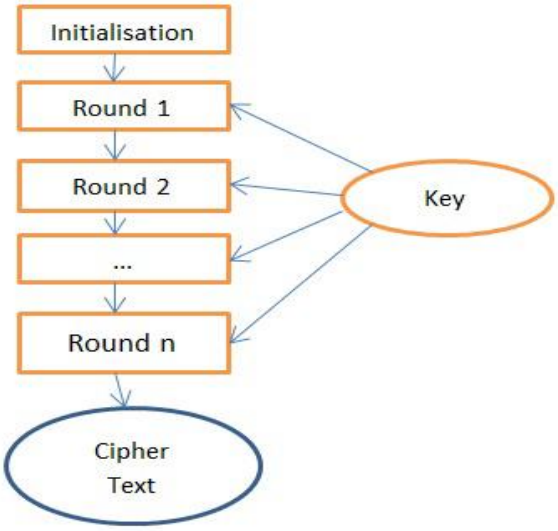

Figure 5.1 Overview of Data Encryption Standard

5.2 WHIRLPOOL

WHIRLPOOL is a hash function designed by Vincent Rijmen and Paulo S. L. M. Barreto that operates on messages less than 2256 bits in length, and produces a message digest of 512 bits. Historically, WHIRLPOOL had three versions. The first version, WHIRLPOOL-0, was submitted to the NESSIE project. Its ”tweaked” successor, WHIRLPOOL-T, was selected for the NESSIE portfolio of cryptographic primitives. A flaw in its diffusion layer reported by Shirai and Shibutani (”On the diffusion matrix employed in the Whirlpool hashing function,” NESSIE public report, 2003) was fixed afterwards, and the final version (called simply WHIRLPOOL for short) was adopted by the International Organization for Standardization (ISO) in the ISO/IEC 10118-3:2004 standard. WHIRLPOOL uses Merkle-Damgrd strengthening and the Miyaguchi-Preneel hashing scheme with a dedicated 512-bit block cipher called W. This consists of the following. The bit string to be hashed is padded with a lquo;’1’-bit, then with a sequence of ’0’-bits, and finally with the original length (in the form of a 256-bit integer value), so that the length after padding is a multiple of 512 bits. The resulting message string is divided into a sequence of 512-bit blocks m1, m2,... mt which is then used to generate a sequence of intermediate hash values H0, H1, H2, ... Ht. By definition, H0 is a string of 512 ’0’-bits. To compute Hi, W encrypts mi using Hi-1 as key, and XORs the resulting ciphertext with both Hi-1 and mi. Finally, the WHIRLPOOL message digest is Ht.

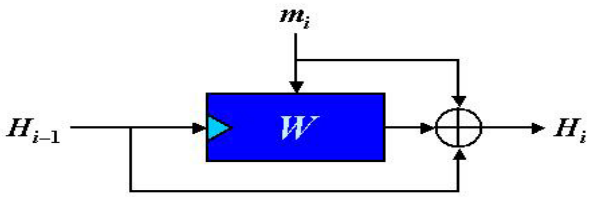

Figure 5.2 Miyaguchi-Preneel Scheme

The W block cipher used by WHIRLPOOL is very similar to the AES algorithm, RIJNDAEL, the main differences being sketched in the following table: The coding for this algorithm is very much similar to that of AES.The W S-box, which in the original submission is generated entirely at random (i.e. lacks any internal structure), by a recursive structure: the new 88 substitution box is composed of smaller 44 ”mini-boxes” (the exponential E-box, its inverse, and the pseudo-randomly generated R box). The coding for the algorithm involves the following steps.

5.2.1 Initialisation Function

The initialisation function given below creates a basic hashing state for each new input given. The hashing state defines a basic skeleton for the hashing function.

5.2.2 Addition Function

The snippet shown below declares the position of the pointers in the plain text. A buffer is also created. Also the data is processed 8 bit at a time. Before this process the data is split into blocks in such a way that each block has 512 bits. The last block is padded at the end with zeroes.

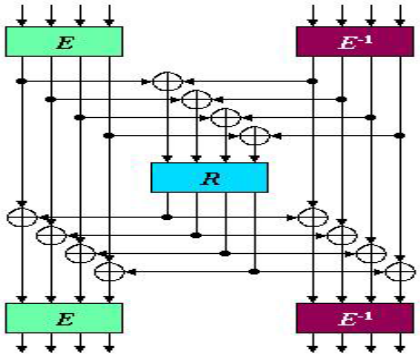

Figure 5.4 Tweaked S-Box Preparation

5.2.3 Finalising Function

The function given below generates the 512 bit cipher text by processing block by block. The above function also makes use of the miyaguchi-preneel scheme of cipher text generation.

VI. PERFORMANCE ANALYSIS

Let K1, K2 denotes the keys in the key pool.
Let Ks, Km denotes the number of keys in the static and mobile key pool.
DK1,K2 denotes the data transfer using the keys K1 and K2.
Access point involved in data transmission picks a key K1 from the Ks number of keys in the static pool and a key K2 from the Km number of keys in the mobile pool.
Selecting a key from the static key pool: Ks C1
Probability of choosing a key from the static key pool, PK1 = 1/Ks C1
Selecting a key from the mobile key pool: Km C1
Probability of choosing a key from the static key pool, PK2 = 1/Km C1
Let PCC denotes the probability of arriving at the correct combination of keys.
Let S denotes the strength of the algorithm which depends on the length of the key, length of the encrypted text and the encrypted mechanism.
Let Pbef denote the probability of access point replication attack before separation of layers.
Pbef = (1/Ks C1) + (1/Km C1) + PCC + S …(1)
Let Paft denote the probability of access point replication attack after node separation.
Direct contact nodes will share the key only from the static key pool. Let x be the small percentage of the keys gets added to the mobile key pool(Hybrid key pool)
Selecting key from the static and mobile key pool,
Y = (Km C1) * (x C1)
Paft = (1/Ks C1) + (1/Y) + PCC + S …(2)
Comparing (1) and (2), its clear that
Paft << Pbef

The factor 1/Y slightly less than 1/Km C1 which makes Paft to decrease, therefore the probability of attack after the node separation is reduced. Even though, an attacker creates the node, the chance of getting the correct combination of these is difficult i.e the attacker has to search for the correct combination of keys over large coverage of nodes. Since the keys are altered, it becomes a difficult task for the attacker to retrieve the data transferred in the network. A graph is plotted with Pbef on the Y axis and the trial number on the X axis.

From equation number 2 we then calculate Paft. A graph is also drawn with Paft on the Y axis and Trial Number on the X axis.

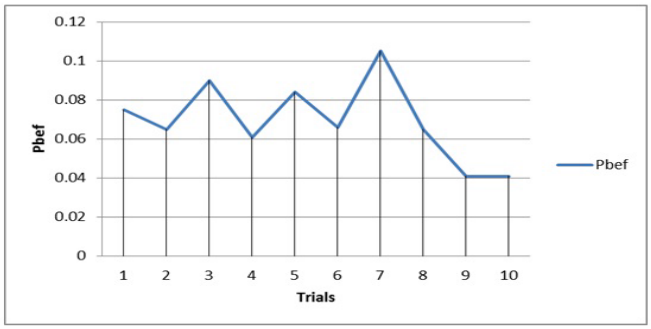

Figure 6.1 Graph of Proposed Probability Pbef

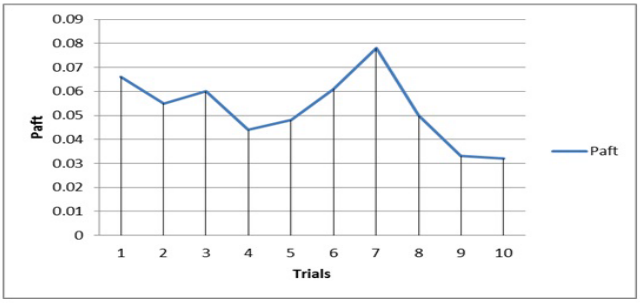

Figure 6.2 Graph of Enhanced Probability Paft

VII. CONCLUSION

The enhanced three-tier security framework has increased the security between sensor nodes and mobile sinks. By splitting the access point layer, we have achieved more resilience and protection against access point and mobile sink replication attacks. Analysis indicates that after separation of layers and key distribution, the probability of access point replication attack is reduced. The proposed scheme on polynomial pool based key pre distribution substantially improved the network resilience to mobile sink replication attacks compared to single polynomial pool based scheme. We have further improved the security performance of the proposed scheme against access point replication attack by strengthening the authentication between access nodes and mobile sinks.

7.1 FUTURE WORK

Although the enhanced three tier security scheme is more resilient towards access point replication attack, it is weak against wormhole attack. As time progresses, more type of threats will haunt WSNs. So, more complex security frameworks and stronger authentication schemes should be developed.

REFERENCES

[1] R.Mahapatra A.Rashid, "An efficient key distribution scheme for establishing pairwise key in distributed sensor networks", Proceedings of IEEE, , 2008.
[2] R.Mahapatra A.Rashid, "A key predistribution scheme for heterogenous sensor networks", IEEE Conference, 2009.
[3] R.Mahapatra A.Rashid, "The three tier security scheme in wireless sensor networks with mobile sinks", IEEE transactions, vol. 23, num. 5, pp. 958–965, 2012.
[4] L.Lamport, "Password authentication with insecure communication", Comm.ACM, vol. 24, num. 11, pp. 770–772, 1981.
[5] M.Praveen Kumar Naregalkar Akshay, "An efficient approach for sensor deployments in wireless sensor network", IEEE conference, 2011.
[6] Mustafa M. Matalgah Walid Y. Zibideh, "Modified-des encryption algorithm with improved ber performance in wireless communication", IEEE conference, 2011.
[7] E.Cayirci Y.Shankarasubramaniam, "Wireless sensor networks: A survey", Proceedings of the IEEE, vol. 38, num. 4, 2002.
[8] Wen Tao Zhu, "Node replication attacks inwireless sensor networks: Bypassing the neighbor-based detection scheme", IEEE conference, 2011.