International Journal of Application or Innovation in Engineering & Management (IJAIEM)
Web Site: www.ijaiem.org Email: editor@ijaiem.org
Volume 4, Issue 6, June 2015 **ISSN 2319 - 4847**

Energy Efficient and Dynamic Key Management Scheme for Wireless Sensor Networks

C.Krishna Priya[1], Prof. Bachala Sathyanarayana[2]

[1]Research Scholar, Department of Computer Science and Technology,
Sri Krishnadevaraya University.

[2]Professor, Department of Computer Science and Technology,
Sri Krishnadevaraya University.

ABSTRACT

In Wireless Sensor Networks, efficient key management plays a vital role in secure communications. Unlike their wired counterparts, WSNs are vulnerable to attacks due to open network architecture, highly dynamic network topology besides their resource constrained nature. As WSN became ubiquitous, it is inevitable to have efficient key management scheme. Moreover, in hostile environments the nodes in WSN are vulnerable to security risks due to dead nodes problem and probability of node capture. Security mechanisms used in traditional networks are not suitable for WSN. Energy efficient dynamic key management scheme is essential for ensuring fool proof security in WSN. There are many existing key distribution schemes for WSN in the literature. However, most of them are static in nature. In this paper we explore a dynamic key management scheme for WSN. We used cluster-based sensor network for implementing key management scheme. Public Key Cryptography is used for the proposed key management scheme which is based on broadcast authentication. The proposed scheme can efficiently handle attacks launched by adversaries besides ensuring that dead nodes cannot cause security leaks. Since energy is a valuable resource for WSN, our scheme is made energy efficient. The proposed scheme can also handle compromised cluster head efficiently. Simulation results reveal that the proposed scheme is energy efficient and supports dynamic key management in dynamic network environment for high level of security.

Index Terms:-Wireless Sensor Network (WSN), security, key management, energy efficiency

1.INTRODUCTION

Wireless networks such as WSN are growing rapidly as they have utility in the real world applications in both civilian and military. WSN is made up of nodes that are configured without cable and they are meant for sensing data around them. Thus these networks became popular for a variety of applications. The nodes in the network have wireless communications, power of computing, power of perception, collaboration, capable of covering large geographical areas in order to monitor surroundings. Especially in the areas where humans cannot monitor, these networks are handy. These networks can be of two varieties namely static and dynamic. The former model deploys static nodes in the fields and they do not move in the field.. The latter on the other hand is deployed in dynamic environments where mobility of sensor nodes is given importance. These networks are self-organizing and making rapid strides into various fields. The applications of dynamic WSNs include transport, logistic services and healthcare devices or wearable devices that monitor vital signs of patients to have an early detection and alert system which helps the health care domain to improve services. Other fields in which dynamic WSN is essential include monitoring of wild life habitat, monitoring enemy territory in military, and monitoring the possibility of natural disasters. These real time applications make the WSNs attractive and very useful.

There are certain inherent issues with WSN. They include that the nodes in the network are deployed in dangerous environments; the nodes are having mobility; nodes have limited energy resources; nodes are vulnerable to various security attacks. In order to protect WSN from attacks and make them energy efficient as well many schemes came into existence. Related Works section of this paper throws light on them. However, most of the schemes are static in nature and they can't cope with the dynamic nature of the modern WSNs.

In this paper, we propose a scheme which is suitable for dynamic WSNs for efficient key management. The scheme also helps in efficient energy utilization. The scheme supports security mechanisms like authentication and dynamic update of the data structure that holds security information. The scheme works in two different phases namely initialization phase and running phase. The real time updating of keys in the proposed system is the key for the success of secure key distribution in wireless networks. The proposed scheme can also handle compromised cluster head efficiently. Simulation results reveal that the proposed scheme is energy efficient and supports dynamic key management in dynamic network environment for high level of security. Our contributions in this paper are as follows.

- We proposed a key management scheme that is both energy-efficient and secure.

- The model is suitable for dynamic WSNs where the periodic key update is essential due to node mobility. Our mathematical model is supported by security analysis.

The remainder of the paper is structured as follows. Section 2 reviews literature on secure key distribution mechanisms. Section 3 presents an overview of the proposed approach. Section 4 provides security and performance analysis while section 5 concludes the paper besides making recommendations for future work.

2.RELATED WORKS

Cryptography has been around for many years for securing communications over networks. Due to the developments in technologies, cryptography also witnessed growth in practice and theory. Many techniques in cryptography came into existence to suit the needs of various systems or networks. For instance, symmetric cryptography, asymmetric cryptography, quantum cryptography etc. are some of the developments in cryptography. All the algorithms or techniques that are available to secure systems have their own strengths and weaknesses. However, in this paper we are finding a suitable one for efficient key management in WSN. Not only security but energy consumption has to be kept in mind with respect to WSNs. This is because they are energy constrained and needs to efficiently utilize energy for longevity of network.

2.1Existing Key Management Schemes in WSNs

The key management schemes in WSN can be divided into three categories. They are actually explored in [2]. They include random key pre-distribution type, self-protected type, and trusted server based. With respect to trusted server-based schemes the credibility of server is an issue. One has to assume that trusted server is highly secure in nature. This assumption can't be used in the real world applications of WSN. For this reason this is not widely used scheme in WSN. The self-protected model on the other hand makes use of cryptographic algorithms such as RSA which is a kind of asymmetric encryption standard. However, this kind of encryption causes overhead on the network and naturally causes more energy to be consumed. Since it is not energy efficient, it is not used widely. The other scheme is random key pre-distribution. This kind of key management scheme is widely used. In this scheme the key generation and usage is done in distributed fashion. Therefore this scheme provides more security than the other two schemes. However, its drawback is that it is suitable for static networks. This is not the case with real world applications where WSNs are highly dynamic in nature.

Per rig et al. [3] proposed SPINS which is a trusted server based solution. It makes use of two protocols namely TESLA and SNEP. The former is used for radio certification while the latter is used for secure communication. The SPINS approach is that a key is known to every sensor node and its corresponding key is maintained by the base station. During broadcast one way hash function is used for authentication. In this approach having a direct connection and communication between two nodes is not advisable for security reasons. Eschenauer and Gligor [4] presented a pre-key distribution model which provides secure communications and energy is efficiently managed. In this scheme, the setup phase ensures that each node in the network is given keys and two nodes will share one of the keys. When compared with the model presented in [3], this model does not use a base station to have secure communication. Based on this model Chan, Perrig and Song [5] introduced the concept known as "q-composite" where q keys are shared between two nodes in the network for direct communication. This ensures more connectivity in the network and increased security with desirable resistance to attacks. Storing large number of keys and maintaining them is the limitation of this scheme due to overhead in memory usage. Liu [6] introduced a key pre-deployment scheme in association with another scheme proposed in [7] to promote node connectivity and reduce memory usage.

Later on Zhang [8] proposed NPKPS that is a pair-wise key distribution scheme which is in a position to provide better security and connectivity besides energy efficiency when compared with the scheme explored in [9]. Security certificate and security key for key management concepts were introduced in [10] and [11] for secure authentication scheme in WSN. This scheme also proved to be energy efficient. Kim [12] proposed a new scheme known as layer-based multiplex communication key management which reduced overhead in communication. Based on this scheme Chuang [13] explored clustering and node mobility. Polynomial key distribution concept was explored in [14] for key-pre distribution. Real time key generation and reduction in memory consumption was focused in [15] for secure communications in WSNs. A key distribution method was proposed in [16] by Camtepe and Yener which was later improved in [17] which improved physical connectivity and direct pair-wise communication among sensor nodes. Key management scheme with server support was introduced by Maerien [18] in which each node in the network is assigned a symmetric key which is also shared with server. However, it assumes mutual trust between the nodes and server.

A key management scheme which is heterogeneous network-aware was proposed in [19] which is efficient in energy consumption and key management, mobility and connectivity. However, its drawback is that it is not able to update keys in real time. This causes it not to be satiable for networks where real time update of keys is essential. Thus WSN has got rapid strides in improvements and security schemes. Most of the schemes in the literature are suitable for static WSN. In this paper we build a scheme for dynamic network and the scheme is expected to be energy-efficient and highly secure.

3.PROPOSED KEY MANAGEMENT SCHEME

In this section we introduce our scheme for key management. The scheme has phases such as network initialization and key establishment. Prior to the description of the proposed scheme, here are the assumptions made to complete the scheme.

- There is synchronization of timing of sensor nodes with each other.
- Base station is in a secure place which possesses unlimited resources like memory and computational power.
- The base station is equipped with intrusion detection mechanism

3.1Architecture of Proposed Scheme

The runtime overview of the proposed key management scheme is described here. The flow of the scheme is illustrated in Figure 1. The WSN considered is with clusters. Each cluster has a cluster head. Two users are considered as Alice and Bob. There is secure communication among the nodes with the proposed scheme.

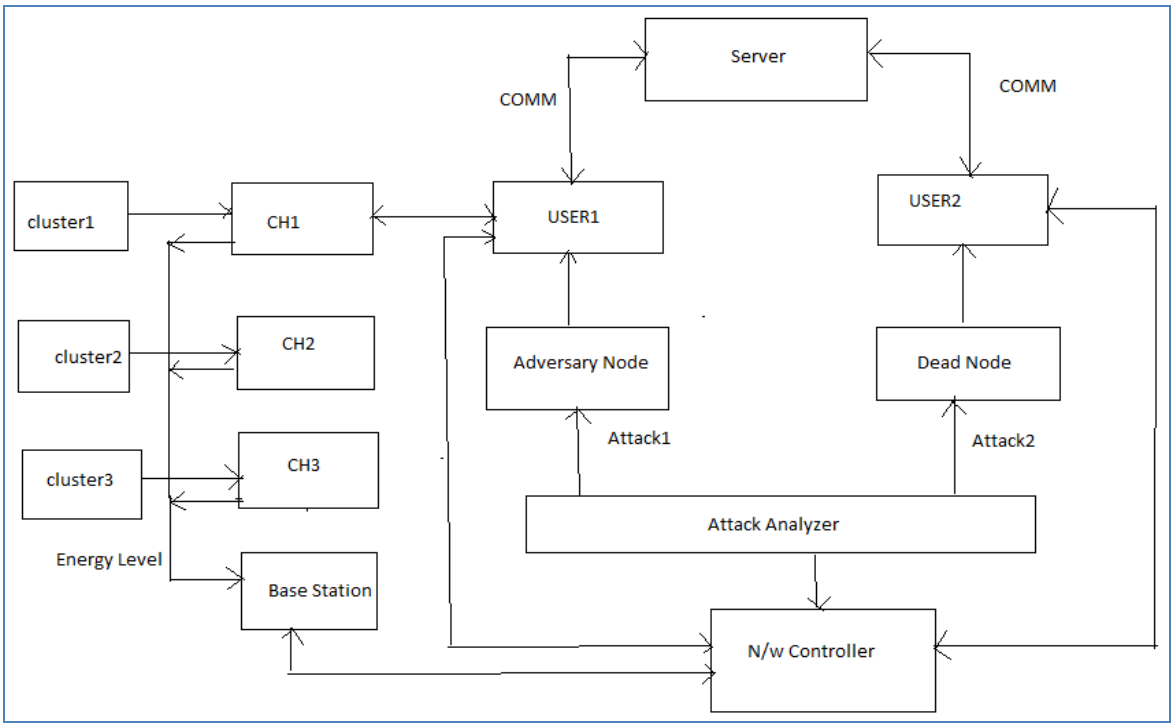

Figure 1 – Architectural overview of the proposed scheme

The nodes in a cluster share a key known as cluster key which is meant for broadcasting messages securely. This key can be updated by cluster head when new sensor joins the cluster or an existing node leaves the cluster. Cluster heads forwards data to base station. The cluster keys are communicated to base station through network controller. Based on the messages exchanged with base station, the cluster keys are updated. Each node in the network shares different pair wise key with neighbours for secure authentication and communication in the network. Nodes can dynamically establish pair wise key between other nodes in the network using public key cryptography.

3.2Network Initialization

The BS is the first layer which controls the network and also helps in connecting WSN to external networks like Internet. The second layer is known as CH layer. The CH is coordinates all other nodes in the cluster in terms of data transfer and other operations. The third layer is meant for collecting data from surrounding environment and sends that to cluster head. The SN layer is divided into many portions known as clusters. Each cluster has a CH which coordinates all SNs in the cluster. The SNs can communicate with other SNs in the same cluster and also the CH. All CHs of all clusters can communicate with each other and also the BS. The proposed scheme makes use of two kinds of keys for encryption. Out of them, the first one is a shared key between CH and SNs while the second one is the master key shared between BS and CHs. The master key is divided into many sub keys which are distributed among the CHs dynamically. CH has more energy consumption due to its heavy responsibilities. Our scheme can balance energy consumption by rotating CHs randomly. The notation used in this paper is presented in Table 1. Before the WSN is actually deployed each node is given a random number for identification and also a secret key is shared with BS. Then the rest of the process is as follows.

Step 1

Whenever CHs are selected randomly, the initial key is used by them to encrypt messages and send to BS to notify that they became CHs.

$$CH_k \rightarrow BS: E_K[M \| T \| ID_k]$$

On the other hand, SNs can also send message to BS in similar fashion.

$$SN_{kl} \rightarrow BS: E_K[T \| ID_{kl}]$$

Table 1 – Notations used in the scheme

CH_k	Cluster head of the *k*th cluster
ID_k	The identity of CH_k
SN_{kl}	The lth sensor node of kth cluster
ID_{kl}	The identity of SN_{kl}
K	The initial key stored in each node
CHK_{kl}	The Key shared between SN_{kl} and CH_k
BSK	The master key shared between CHs and BS
y_k	The sub key of CH_k
x_k	The session of CH_k
$E_K[M]$	The symmetric encryption for *M* using key *K*
$D_K[M]$	The symmetric decryption for *M* using key *K*

M and T represent message of CH and timestamp respectively.

Step2

BS divides the WSN based on the distance between itself and SNs and sends identity list of sensor nodes to every CH in the network.

$$BS \rightarrow CH_k: E_K[M \| ID_{list}]$$

$$ID_{list} = (ID_{k1}, ID_{k2}, ID_{k3}, \ldots, ID_{kn})$$

Where *M* is the message of SNs,

Step 3

When CH receives a message, it is broadcasted to SNs in order to let them join the cluster. This way clustering process is finished.

3.3Key Establishment Phase

3.3.1Cluster Key Establishment

Once network initialization is completed, each SN is responsible to establish secure communication to CH and other SNs in the same cluster. It is done using the steps given below.

Step 1

In the beginning a random number *i* is chosen by BS encrypts it with initial key K and sends that to all nodes.

$$BS \rightarrow SN_{kl}: E_K[M \| i]$$

$$BS \rightarrow CH_k: E_K[M \| i]$$

Where M is the message of the random number.

Step 2

Upon receiving the random number, a key is generated as follows and that is shared between CH.

$$CHK_{kl} = h(i + ID_{kl})$$

Step 3

If the sender node, denoted as SN_{kl} wants to exchange information with other node, denoted as $SN_{k(l+1)}$, it is supposed to use CHK_{kl} to encrypt that information before transmitting it along with identity ID_{kl} to $SN_{k(l+1)}$.

$$SN_{kl} \rightarrow SN_{k(l+1)}: ID_{kl} \| E_{CHK_{kl}}[M]$$

Where M represents the information being exchanged.

Step 4

Identity of SN_{kl} , $SN_{k(l+1)}$ and hash function are used to find out x and then the message is decrypted.

Step 5

Once cluster key establishment is finished, the initial key K shared with BS is deleted by each SN.

3.4Master Key Establishment

Each CH in the WSN has a pre-loaded initial key that has been shared with BS. In case of attacks launched by adversary, the CH reveals all messages when there is no change in the initial key. Therefore it is necessary to change the master keys between BS and CHs. It is achieved by using the steps as follows.

Step 1

First of all, base station selects t-1 integers such as $r_1, r_2, r_3, \ldots \ldots, r_{t-1}$ randomly and builds r (t - 1)th degree polynomial as follows.

$$f(x) = BK + r_1 x + r_2 x^2 + \cdots + r_{t-1} x^{t-1}.$$

In order to secure communication between CHs and BS the master key BK is used.

Step 2

BS is able to use identities of CHs and I in order to compute y_k which is the sub key of CH_k where

$$y_k = f(i + ID_k),\ 1 \leq k \leq m;$$

m denotes the number of CHs. The BS uses initial key K for encrypting yi and then sends it to CH_k.

$$BS \rightarrow CH_k : E_K[M \| y_k]$$

Where M refers to message pertaining to key updating.

Step 3

On receiving message, CH_k deletes the initial key and uses x, hash function and *i* in order to generate x as a session key with other cluster heads in WSN where

$$x_k = h(i + ID_k).$$

Step 4

Once the CH_k receives information from SNs, it fuses such information and transmits to base station. As per the threshold secret sharing scheme (t,n), CH_k should be able to get sub keys of other t-1 CHs so as to enable it to reconstruct master key. Towards it, CH_k sends a request to BS.

Step 5

Afterwards, the base station randomly selects t-1 CHs and sends them the reconstruction details and the identity of CH_k which is encrypted using the initial key K.

$$BS \rightarrow CH_{\tilde{k}} : E_K[M \| ID_{\tilde{k}}]$$

Step 6

On message is arrived at CH_{k+1}, it makes use of a sub key x and encrypts they sub key y_{k+1} and then sends it to CH_k along with its identity ID_{k+1}.

$$CH_{K+1} \rightarrow CH_k : ID_{k+1} \| E_{x_{k+1}}[M \| y_{k+1}]$$

where M pertains to the message of reconstruction of master key. That way CH_k can configure x_{k+1} and decrypt the message besides getting y_{k+1}.

Step 7

On receiving t-1 sub keys, master key BK is constructed by x and shared with BS. Afterwards t-1 sub keys are received, the reconstruction of master key BK is done by x which is shared with base station. Then initial key is deleted and master key BK is used to establish secure communication with base station.

3.5Key Updating

3.5.1Periodic Key Updating

As part of the dynamic key management scheme in the event of network existence for some time, keys are updated by the BS so as to avoid adversaries from successful launch of attacks. In the proposed scheme BS is supposed to change random number *i* for the purpose of updating keys associated with nodes. The whole mechanism is as follows.

Step 1

BS, first of all, selects a new random *i* and a new master key denoted as BK. Afterwards, the BS new sub keys are constructed by BS and sent to CHs in WSN.

$$BS \rightarrow CH_k : E_{BK}[M \| i \| y_k]$$

where M represents the message of updating and

$$y' = f(i' + ID_k),\ 1 \leq i \leq m;$$

Step 2:

After that, each CH uses the shared key with SN to encrypt the new random number, and transmits it to its cluster members.

$$CH_k \rightarrow SN_{kl} : E_{CHK_{kl}}[M \| i]$$

Step 3:

Then all SNs use i' to recalculate the new shared keys CHK'_{kl} shared with their CH. And CHs compute new session keys in the same way, where

$$CHK_{kl} = h(i + ID_{kl})$$

$$x_k' = h(i' + ID_k)$$

Step 4:

After doing that, all the nodes delete the initial key information. In this way, BS can update all shared keys only by changing the random number. Thus one process of key updating is finished.

1) Node addition and deletion: When a SN is added in the network field, BS will transmit the current random number to it. And SN can establish secure communication with its CH, only after calculating the key shared with it. On the other hand, if BS detects out that a SN is captured by adversaries or exhausts energy, it will inform the CH of failure SN. Then the CH will broadcast that the SN is invalid and delete its identity. Since that each SN has a unique key shared with the CH, and SN's compromise won't reveal the communication between other nodes. So there's no need to update the keys.

2) CH replacement: According to LEACH, a cluster head election algorithm quoted in our protocol, nodes are randomly selected as CH and rotated so as to balance the energy dissipation in WSN. Once a new CH is selected, BS must renew keys to ensure the security of network. It only needs to broadcast the message to the SNs in its cluster and notice BS to trigger the key update mechanism to refresh the keys.

In addition, if BS detects out that a CH is captured, it will inform the SNs of this cluster and other CHs, and trigger the key update mechanism immediately.

4.SECURITY AND PERFORMANCE ANALYSIS

4.1Security analysis

Our protocol adopts the conception of threshold secret sharing scheme, dividing the master key into several sub keys. Each CH only stores the sub key instead of the master key used to encrypt data. As long as the attacker captures fewer than *t* CHs, it cannot reconstruct the master key S. Besides, BS triggers key update mechanism regularly to refresh the key information. So even if the attacker captures *t* CHs of different time quantum, it also can't reconstruct the master key. In our scheme, since the key shared between SN and CH is generated by its identity, each SN has a unique shared key with its CH. So, any SN's compromise won't affect the secure communication between other SN and CH. Moreover, if any CH is captured or exhausts energy, the BS will refresh the key information in the network, and the keys stored in those abandoned nodes are useless. Conclusively, our scheme provides sufficient security and can achieve perfect compromise resilience.

4.2Dynamic analysis

To ensure the security of WSN, we adopt the key update mechanism to make BS update the keys dynamically. In our scheme, by changing the random number *r*, BS can update all the key information and have no need to reselect all keys and polynomial. The SN can generate the shared key by itself, BS has no need to update the old keys and it won't affect secure communication between CH and other sensor nodes. Therefore, our protocol can well meet the demands of the dynamic of WSN.

4.3Overhead analysis

To recover the master key shared with BS, the CH should use the sub keys of any other *t*-1 CHs to reconstruct the master key. According to the Lagrange interpolation polynomial, it is easy to get the master key *S*, where

$$S = \sum_{k=1}^{t} y_k \prod_{l=1, l \neq k}^{t} \frac{ID_l + i}{ID_l - ID_k}$$

So the computational complexity of the master key reconstruction is $O(t3)$. As to SNs, the shared keys are generated by preloaded one-way function and identity and the random number *r*. Each SN only needs to compute a one-way function algorithm to produce a shared key, and its computational overhead is very low.

In our method, each SN only stores its identity, preloaded one-way function and the initial key shared with BS. And to each CH, it is no need to store all shared keys with its SNs, because that it can get the keys from their identities. In addition, due to the limitation of the node's power and memory, CHs use their session key to encrypt the messages when they want to communicate with other CHs. They don't need to store other CHs' session keys and can figure them out by their identities and the one-way function. According to threshold secret sharing scheme, thought the increase of *t* can reduce the probability of getting the master key, it also cost more time to generate the keys. So, when used in practical application, we must choose an appropriate threshold to keep a good balance between the security and the overhead. Based on these reasons, we can say that our protocol provides low computational overhead and storage.

4.4Simulation and Results

Simulation study has been made in order to realize the proposed approach for efficient key management. The simulation environment is as given below.

Table 2: Simulation environment details

PARAMETER	***SPECIFICATION***
Simulation tools used	NS2 Network Simulator (ns-2.35)
Simulation time	10 sec, 20 sec, 30 sec
Number of nodes	10,20,30
Transmission range	250m
Maximum speed	0-20 m/sec
Application traffic	CBR [constant bit rate] [20]
Packet size	512bytes
Node mobility model	8 packets/sec
Protocol	AODV

The simulation results pertaining to performance level of the proposed method and the other attributes like packet delivery ratio, packet delay and packet dropping were recorded. The results are as shown below.

Table 3: Simulation results

Performance analysis on delay								
	1	2	3	4	5	6	7	8
Existing [20]	26	24	22	20	19	15	10	8
Proposed	24	20	15	11	10	8	5	2
Performance level of packet delivery								
Existing [20]	0.2	0.6f	0.75	0.95	1.5	2.75	3.8	5.85
Proposed	0.5	0.9	2.65	3.75	6.8	8.84	9.9	12.96
Performance on dropping								
Existing [20]	30	28	25	22	18	15	12	9
Proposed	28	26	22	19	17	22	9	5
Network output								
Existing [20]	1	2	3	4	5	6	7	8
Proposed	2	5	6	8	9	10	11	12

Energy Consumption								
Proposed	0.4	0.8	1.25	1.55	2.5	3.75	4.5	6.88
Existing [20]	1.5	2.9	3.65	4.75	6.8	8.84	9.9	10.96

As can be seen in Table 3, it is evident that the simulation results pertaining to delay performance, packet delivery ratio, packet dropping, throughput and energy consumption.

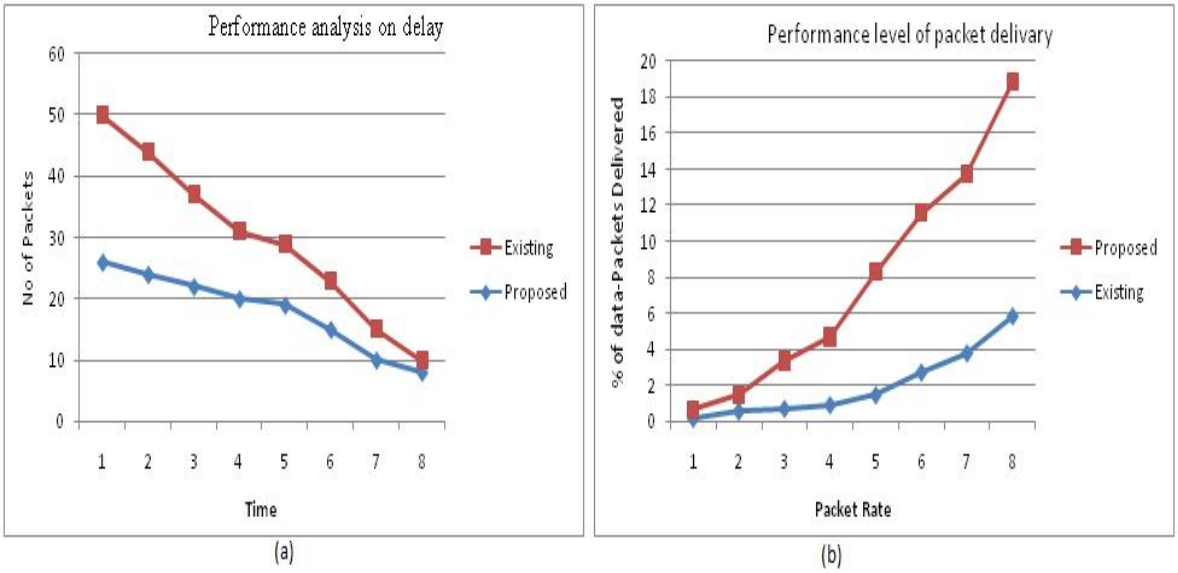

Figure 3 – Results of the proposed approach

As seen in Figure 3 (a), it is evident that the horizontal axis represents the time while the vertical axis represents no. of packets. With respect to the delay analysis, the proposed system exhibits better performance than the existing system. As shown in Figure 3 (b) the packet delivery ratio of the proposed scheme is higher than the existing method.

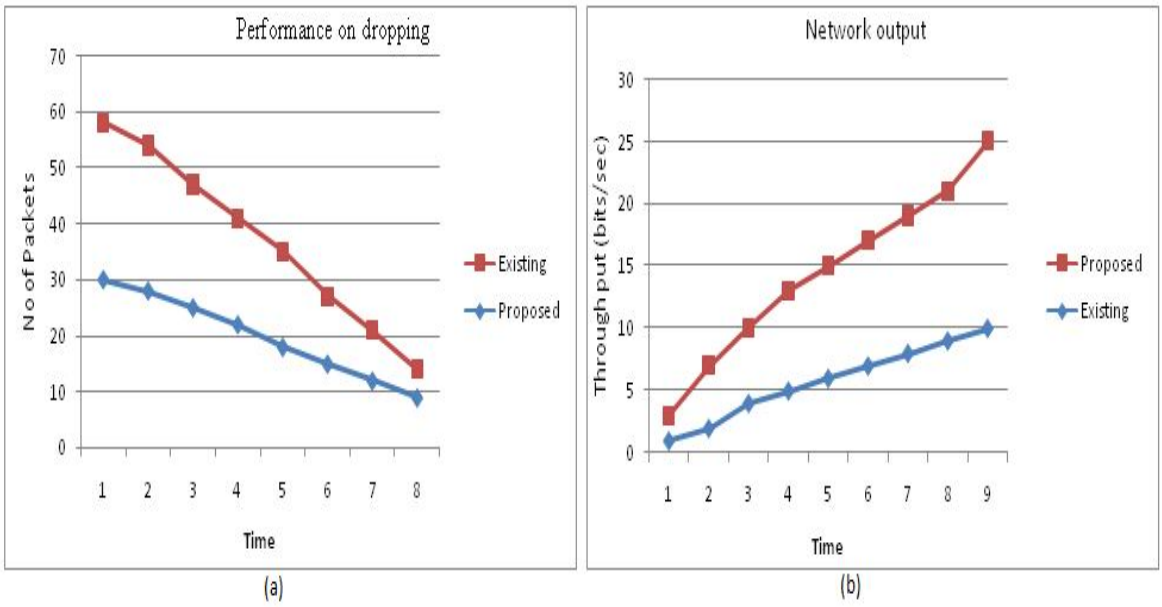

Figure 4 – Performance of the proposed system

As seen in Figure 4 (a), it is evident that the horizontal axis represents the time while the vertical axis represents no.of packets. With respect to the dropping of packets, the proposed system exhibits better performance than the existing system. As shown in Figure 4 (b) the throughput of the proposed scheme is higher than the existing method.

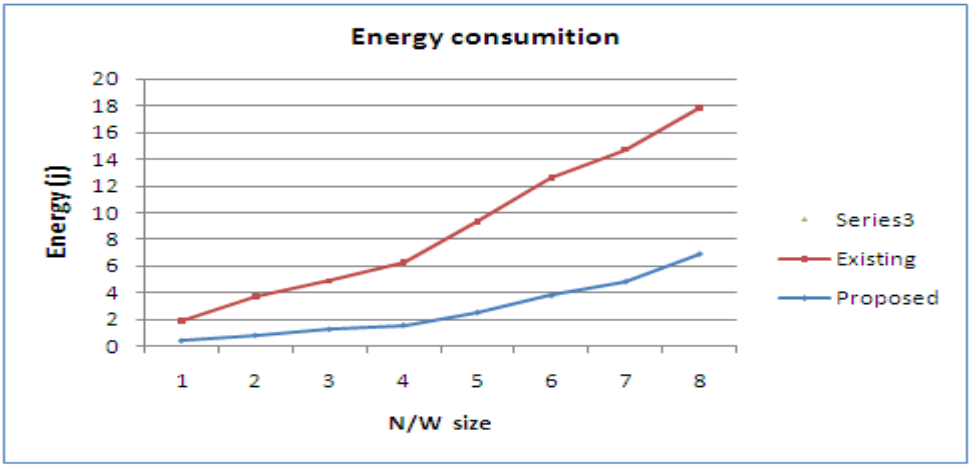

Figure 5- Energy consumption

As seen in Figure 5, it is evident that the horizontal axis represents the network size while the vertical axis represents the energy consumed. As the network size increases, the energy consumption increases in general. The results reveal that the proposed scheme is energy efficient when compared with its prior method.

5. CONCLUSIONS AND FUTURE WORK

In this paper we studied secure key management schemes in Wireless Sensor Networks. As these networks are widely used in the real world, security plays an important role. Secure communication among the nodes in the network is to be given paramount importance as these networks are vulnerable to attacks due to their mobility nature and resource constrained nature. In providing secure communications, key management and key distribution play a pivotal role. Towards this end many schemes came into existence. However many of them are static in nature. They cannot cater their services to dynamic WSNs. In this paper we proposed a key distribution scheme which makes communications over WSN secure in an energy efficient fashion. Our scheme is applied to a SN with CH, BS and sensor node. The proposed mathematical model is supported by the security analysis. The proposed key management scheme is highly secure and energy efficient. The proposed scheme can also handle compromised cluster head efficiently. Simulation results reveal that the proposed scheme is energy efficient and supports dynamic key management in dynamic network environment for high level of security. This research can be extended further by modelling various attacks, evaluating and enhancing so as to ensure that the scheme is robust to those attacks.

REFERENCES

[1] N. Sultana, K. -m. Choi and E. -n. Huh, "Mobility Support Secure Coverage Protocol for Monitoring Applications using Wireless Sensor Network", International conference on Computational Sciences and its Applications ICCSA, (2008).
[2] W. Du, J. Deng, Y. S. Han, S. Chen and Pr. K. Varshney, "A Key Management Scheme for Wireless Sensor Network Using Deployment Knowledge", IEEE INFOCOM, (2004).
[3] A. Perrig, R. Szewczyk, J. Tygar, Victorwen and D. E. Culler, "Spins: Security Protocols for Sensor Networks", ACM Wireless Networking, (2002) September.
[4] L. Eschenauer and V. D. Gligor, "A key management scheme for distributed sensor networks", Proc. of the 9th ACM Conference on Computer and Communication Security, (2002) November, pp. 41-47.
[5] H. Chan, A. Perrig and D. Song, "Random key pre-distribution schemes for sensor networks", Proc. IEEE Symp on Research security privacy, (2003) May 11-14, pp. 197- 213.
[6] F. Liu, M. J. Rivera and X. Cheng, "Location-Aware Key Management in wireless sensor networks", IWCMC'06, (2006).
[7] M. O. Rabin, "Digitalized signatures and public-key functions as intractable as factorization", Technical Report MIT/LCS/TR-212, Laboratory for Computer Science, MIT, (1979).
[8] J. Zhang, Y. Sun and L. Liu, "NPKPS: A novel pair wise key pre-distribution scheme for wireless sensor networks", IET Conference on Wireless, Mobile and Sensor Networks 2007, (CCWMSN07), (2007) December 12-14, pp. 446-449.
[9] L. Girod, T. Stathopoulos, N. Ramanathan, et al., "A System for Simulation, Emulation, and Deployment of Heterogeneous Sensor Networks", Proc. of ACM SenSys, (2004).

[10] O. Cheikhrouhou, A. Koubaa, M. Boujelben and M. Abid, "A lightweight user authentication scheme for Wireless Sensor Networks", 2010 IEEE/ACS International Conference on Computer Systems and Applications (AICCSA), (2010) May 16-19, pp. 1-7.
[11] H. -R. Tseng, R. -H. Jan and W. Yang, "An Improved Dynamic User Authentication Scheme for Wireless Sensor Networks", Global Telecommunications Conference 2007, GLOBECOM '07. IEEE, (2007) November 26-30, pp. 986-990.
[12] K. T. Kim, R. S. Ramakrishna, "A Level-based Key Management for both In-Network Processing and Mobility in WSNs", IEEE Internatonal Conference on Mobile Adhoc and Sensor Systems, MASS 2007, (2007) October 8-11, pp. 1-8.
[13] I. -H. Chuang, W. -T. Su, C. -Y. Wu, J. -P. Hsu and Y. -H. Kuo, "Two-Layered Dynamic Key Management in Mobile and Long-Lived Cluster-Based Wireless Sensor Networks", Wireless Communications and Networking Conference, WCNC 2007, IEEE, (2007) March 11-15, pp. 4145-4150.
[14] C. Blundo, A. De Santis, A. Herzberg, S. Kutten, U. Vaccaro and M. Yung, "Perfectly Secure Key Distribution for Dynamic Conferences", (1992) pp. 471–486.
[15] S. U. Khan, L. Lavagno, C. Pastrone and M. Spirito, "An effective key management scheme for mobile heterogeneous sensor networks", 2011 International Conference on Information Society (i-Society), (2011) June 27-29, pp. 98-103.
[16] S. A. Camtepe and B. Yener, "Combinatorial Design of Key Distribution Mechanisms for Wireless Sensor Networks", Networking, IEEE/ACM Trans. on, vol. 15, no. 2, (2007) April, pp. 346-358.
[17] D. S. Sanchez and H. Baldus, "A Deterministic Pairwise Key Pre-distribution Scheme for Mobile Sensor Networks", SecureComm 2005, First International Conference on Security and Privacy for Emerging Areas in Communications Networks, (2005) September 5-9, pp. 277- 288.
[18] J. Maerien, S. Michiels, C. Huygens and W. Joosen, "MASY: MAnagement of Secret keYs for federated mobile wireless sensor networks", Wireless and Mobile Computing, Networking and Communications (WiMob), (2010) October 11-13, pp. 121-128.
[19] S. U. Khan, C. Pastrone, L. Lavagno and M. A. Spirito, "An Energy and Memory-Efficient Key Management Scheme for Mobile Heterogeneous Sensor Networks", 2011 6th International Conference on Risks and Security of Internet and Systems (CRiSIS), (2011).
[20] Hamzeh Ghasemzadeh, Mohammad Reza Aref, Ali Payandeh (2000). A novel and low-energy PKC-based key agreement protocol for WSNs adversary. Broadcast Authentication. IEEE, p1-7.

AUTHORS

C.Krishna Priya received her Master of Computer Applications from Sri Krishnadevaraya University, Anantapuramu, A.P., India, in 2007. She is currently pursuing her Ph.D in Computer Science and Technology at Sri Krishnadevaraya University, Anantapuramu, A.P., India. Her current research interest includes Computer Networks

Prof. B.Sathyanarayana received his B.Sc Degree in Mathematics, Economics and Statistics from Madras University, India in 1985, Master of Computer Applications from Madurai Kamaraj University in 1988. He did his Ph.D in Computer Networks from Sri Krishnadevaraya University, Anantapuramu, A.P. India. He has 24 years of teaching experience. His Current Research Interest includes Computer Networks, Network Security and Intrusion Detection. He has published 30 research papers in National and International journals