International Journal of Emerging Trends & Technology in Computer Science (IJETTCS)
Web Site: www.ijettcs.org Email: editor@ijettcs.org
Volume 6, Issue 5, September- October 2017 ISSN 2278-6856

Energy-Aware Robust Key Management Scheme for Dynamic Wireless Sensor Networks

Dr. C.KrishnaPriya[1], **Dr.P.Sumalatha**[2]

[1] Department of Computer Science and Technology, Sri Krishnadevaraya University,
Anantapuramu, Andhra Pradesh, India

[2] Department of Computer Science and Technology, Sri Krishnadevaraya University,
Anantapuramu, Andhra Pradesh, India

Abstract: ***Security of communications over WSN is very important. Unlike their wired counterparts, WSNs throws many challenges apart from resource constrained nature such as open network architecture, highly dynamic network topology. Therefore an energy-aware scheme is required to protect communications. There are many key distribution schemes for WSN are existed in the literature but most of them are static in nature. In this paper we explore a new key distribution scheme for dynamic WSNs. In such network where the nodes are dynamic in nature and nodes have mobility, it is essential to have a mechanism for key updating. This is achieved using a self-organizing binary tree known as AVL tree. This data structure is capable of adapting to the dynamic situations of WSN and updates the key values in real time. We proposed algorithms to achieve this. We also built a prototype application that demonstrates the application of the scheme for secure video distribution in a network. Our empirical results reveal that the proposed scheme is energy efficient and secure.***

Keywords: Wireless Sensor Networks (WSN), Key Management, Energy Efficiency, AVL tree.

1. INTRODUCTION

Wireless Sensor Network (WSN) is growing rapidly as they are widely used in the real world like both civilian and military applications. WSN is comprised of hubs which are arranged without cable and are utilized for detecting information around them. The hubs in the system have remote interchanges, energy of perception, and power of computing, equipped for covering extensive geographical regions so as to monitor the environment. Particularly in the regions where people cannot monitor. WSN can be classified into two types namely static and dynamic. The static model is deployed in an environment where nodes in the field doesn't have mobility i.e., they are fixed. The dynamic model is deployed in an environment where mobility of sensor nodes is given more significance. The applications of dynamic WSNs include home appliance management, logistic and transport services, healthcare devices that monitor vital signs of patients to have an early detection which can be used in health care domain to improve services. Other fields where dynamic WSN is needed includes monitoring enemy territory in military, homeland security, monitoring the possibility of natural disasters and forecasting, monitoring of wild life habitat. These networks are self-organizing thus making rapid strides into various fields

There are certain intrinsic issues with WSN, which include that the nodes in the network are deployed in unsafe environments. As the nodes in WSN are energy constrained and have mobility, nodes are vulnerable to various security attacks. Many schemes came in to existence to make them energy efficient and to protect them from attacks. Existing Works section of this paper tosses light on them. Nonetheless, many of the schemes are static in nature and they can't adapt to the dynamic nature of the advanced WSNs.

In this paper, we propose a new scheme which is suitable for dynamic WSNs for effective key management. The scheme utilizes energy in efficient manner and also supports security mechanism like authentication and dynamic update of the data structure which holds security information. The scheme works in two different phases namely network initialization phase and running phase. The real time refreshment of keys in the proposed system is the key for the success of secure key distribution in wireless networks. We built a prototype application that demonstrates the application of the proposed key management system for secret communication over WSN.

The remainder of the paper is organized as follows. Section II reviews literature on secure key management mechanisms. Section III presents an overview of the proposed approach. Section IV presents the application of the key management scheme for secret communication over network. Section V concludes the paper besides making recommendations for future work

2..EXISTING WORKS

Cryptography has been around for a long time for providing secure communications over networks. Due to the recent advancements in technologies, cryptography also witnessed improvements in practice and theory. Numerous techniques in cryptography came into existence to suit the needs of various frameworks or networks. For instance, symmetric cryptography, public key cryptography, quantum cryptography etc. are some of the advancements in cryptography. All the algorithms or techniques which are available for making secure systems have their own strengths and weaknesses. In this paper we are finding a suitable one which is energy-aware robust key management technique for dynamic WSN. This is because they are energy constrained and needs to effectively use the energy for improving the life span of network.

2.1 Existing Key Management Schemes in WSNs

The key management schemes in WSN can be divided into three types. Those are explored in [1]. They are random key pre-distribution type, self-protected type, and trusted server based. With trusted server-based schemes the validity of server is an issue. One has to expect that trusted server is profoundly secure in nature. This assumption can't be useful in the real world applications of WSN. For this reason this scheme is not widely used in WSN. The self-protected model makes use of cryptographic algorithms such as RSA which is a kind of public key encryption standard. However, this kind of encryption causes networks overhead and more energy consumption, so it is not widely used. The other scheme is random key pre-distribution, the key generation and usage is done in distributed fashion. Therefore this scheme provides more security than the other two schemes so this scheme is widely used. Its drawback is that it is only suitable for static networks. As WSNs are highly dynamic in nature, this is not the case with real world applications.

SPINS proposed by Perrig et al. [2] which is a trusted server based solution, which makes use of two protocols namely TESLA and SNEP. The TESLA is used for radio certification while SNEP is used for secure communication. In SPINS approach a key is known to every sensor node and its corresponding key is maintained by the base station. One-way hash function is used for authentication during broadcasting. In this approach having a direct connection and communication between two nodes is not prudent for security reasons. A Pre-key distribution model which is presented by Eschenauer and Gligor [3] is energy efficient and also provides secure communication. In this scheme, the setup phase guarantees that each sensor node in the network is provided with keys and two nodes will share one of the keys. When contrasted with the model presented in [2], this model does not use a base station to have secure communication. Based on this model the concept known as "q-composite" which is introduced by Chan, Perrig and Song [4] in which q keys are shared between two nodes in the network for direct communication. This provides more connectivity in the network and a high level of security with desirable resistance to attacks. The limitation of this scheme is storing large number of keys and their maintenance lead to overhead in usage of memory.

Later on Zhang [5] proposed NPKPS that is a pair-wise key distribution scheme provides better security and connectivity besides energy efficiency when compared with the scheme presented in [6]. For secure authentication in WSN, security certificate and security key for key management concepts were introduced in [7] and [8] which is proved to be energy efficient. Layer-based multiplex communication key management scheme proposed by Kim [9] reduced communication overhead. Based on this scheme Chuang [10] explored clustering and node mobility.

Polynomial key distribution concept was explored in [11] for key-pre distribution. For secure communications in WSNs, real time key generation and reduction in memory consumption was presented in [12]. A key distribution method was proposed by Camtepe and Yener [13] which was later improved in [14] which improved direct pair-wise communication and physical connectivity among sensor nodes. A key management scheme with server support introduced by Maerien [15] in which each node in the network is assigned a private key which is also shared with server. However, it assumes mutual trust between the nodes and server.

A heterogeneous network-aware key management scheme was proposed in [16] which is efficient in energy consumption, key management, connectivity and mobility. Its drawback is that it is not able to update keys in real time. That means, this is not suitable for networks where real time update of keys is required. Thus WSN has got rapid strides in improvements and security schemes. Most of the schemes in the literature are more suitable for static WSN. In this paper we tried to build a scheme for dynamic network and the scheme is expected to be energy-efficient.

3. THE PROPOSED SCHEME

In the proposed key distribution scheme we consider a typical WSN with sensor nodes with mobility, center sensor node and base station. Base station is assumed to have high level of energy. Center sensor node has more energy when compared to sensor nodes that can move around. Figure 1 shows a typical sensor node deployment.

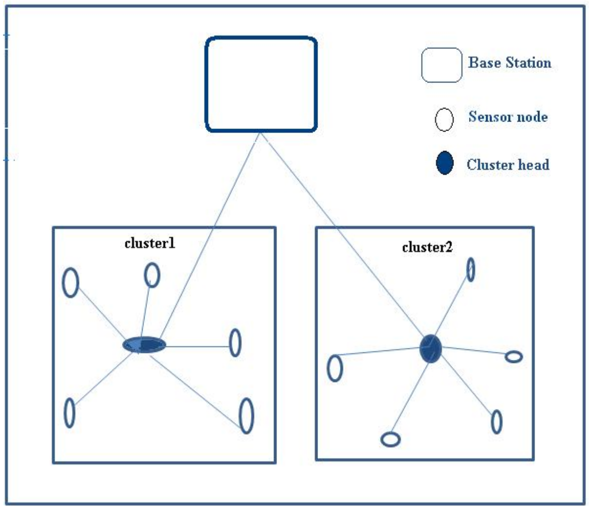


Figure 1 Illustrates WSN

As can be seen in Figure 1, the sensor nodes are connected to a network containing base station, central sensor and other sensor nodes that are responsible to sense data actually

3.1 Initialization Phase

In this phase, the nodes in the network are formed and the details of all the nodes are saved to base station. There are certain activities performed as part of initialization. They include finding energy level of nodes, election of cluster head and cluster formation. First of all energy level of all nodes is computed for further usage of it. There are five levels in energy states namely weakest, weak, strong, stronger and strongest. Zero indicates lowest level while 5 denotes highest level of energy. The energy level of base station is assumed to be 5. For each node the % of residual energy is computed for decisions in the network running phase. Table 1 shows the energy state and corresponding range of percentages of residual energy.

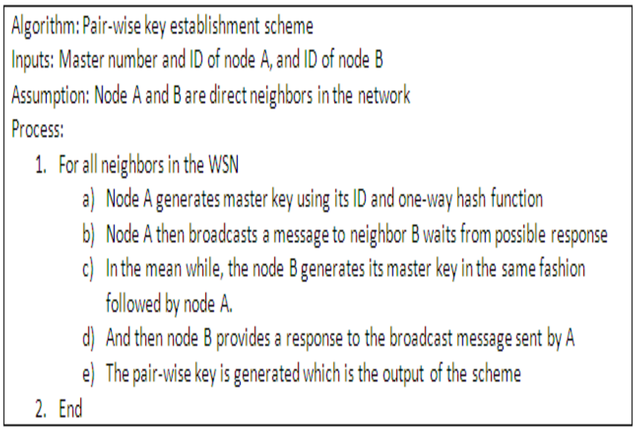
Table 1: Energy states mapped to range of percentages of residual energy

Residual Energy	State
0% -5%	0
6%-20%	1
21%-40%	2
41%-60%	3
61%-80%	4
81%-100%	5

The following are the steps of initialization phase.

1. Computing residual energy levels to know the state of energy of nodes.
2. Base station generates key pairs and public key is distributed to all nodes in the network.
3. All nodes send sample message encrypted with public key to the base station.
4. The base station obtains list of nodes in the network and other information required.
5. On first come first serve basis IDs assigned to each node in the network

After completion of initialization cluster head (CH) election phase is carried out. In this phase, nodes with higher energy are considered and they are elected as cluster heads. The pair wise key establishment between two nodes is done using one-way hash function presented in [17]. The algorithm for pair wise key establishment is as shown in Figure 2



```
Algorithm: Pair-wise key establishment scheme
Inputs: Master number and ID of node A, and ID of node B
Assumption: Node A and B are direct neighbors in the network
Process:
  1. For all neighbors in the WSN
       a) Node A generates master key using its ID and one-way hash function
       b) Node A then broadcasts a message to neighbor B waits from possible response
       c) In the mean while, the node B generates its master key in the same fashion
          followed by node A.
       d) And then node B provides a response to the broadcast message sent by A
       e) The pair-wise key is generated which is the output of the scheme
  2. End
```

Figure 2 Pair-wise key establishment algorithm

As can be seen in Figure 2 the pair-wise key establishment algorithm takes two neighboring nodes' (A, B) ID and master number and produce pair-wise key as output. This is meant for key distribution that is done in the initialization phase. The steps given in the algorithm are repeated for all neighbors. At the end of processing all nodes that have direct neighbor will get pair-wise key. Thus each node in the network can directly compute pair-wise key. After completion of this, cluster formation takes place as follows.

- CH which has been elected sends hello message including its master key encrypted using DES algorithm. The DES algorithm code is available with each node in the network.
- Non-cluster head nodes obtain CH information from multiple nodes. They are aware of multiple CHs. In case if non-cluster head nodes do not get the hello message from CH nodes, they resort to sending hello message with encrypted key and then wait for the response with the intention to know information of CHs.
- Based on the CH information non-cluster head node makes decision to join a cluster. Then the node will send join request to corresponding CH node. The message also contains CHs master number.
- On receiving request, the CH decrypts the message and verifies the new node's validity. If the new node is valid node, the CH will send "confirmation" message which enables the new node to join network. In the verification process, the CH makes use of security primitives being carried into the message to authenticate the user thus preventing replication and replay attacks.
- With the previous step completed, the entire network is formed and ready to serve.

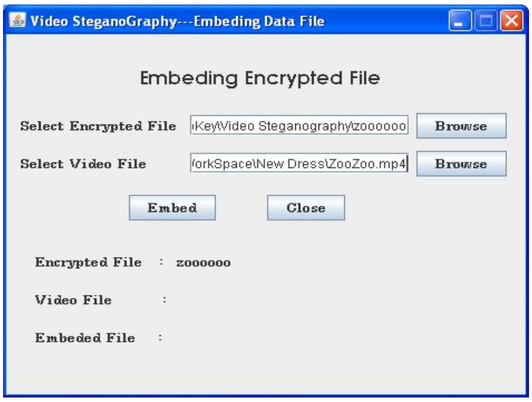
3.2 Network Running Phase

There are two dynamic scenarios in the network at runtime. A new node may join the network and an existing node might move to different cluster. When a new node is willing to join the network, it is possible that base station verifies the master number of the node, and makes decision to allow or deny the node. Once the verification is successful, the base station allocates an ID for the new node which will generally avoid Sybil attack. The new node broadcasts a message in order to get details of all CHs in the network. Then the neighboring nodes take steps to verify the node and replay message. Based on the strength of signal, the new node will join a particular cluster.

Sometimes, the energy of CH comes down beyond specified threshold. In this case, sensor nodes might take decision to join other cluster. When a node needs to move between clusters, it sends a message to find other cluster heads and their energy state. Once CHs respond, based on the energy state the node jumps to corresponding cluster after making a decision by following the procedure described in [16]. After making decision to join the new cluster, the node sends "joining request" to the CH. Then the new CH gets the sensor node's details from original CH and makes a decision to allow the node into its cluster.

4. PROTOCOL APPLICATION FOR SECRET COMMUNICATION

We have considered an application of WSN that enables secret communication over network using the proposed key management scheme presented in the preceding section. In fact we built a custom simulator in Java platform. The prototype demonstrates the embedding and extraction of an encrypted document into or from a video file. This kind of application demonstrates the concept of steganography which is an improved form of cryptography coupled with our key distribution scheme. The prototype is built in such a way that both the information sender and receiver make use of the key distribution mechanism implicitly and ensure highly secure communication between them. The traditional cryptography is used to encrypt or decrypt file to be transferred while the proposed scheme is used for secure key distribution. The encryption phase is as shown in Figure 3. This is done at sender side using the proposed key distribution scheme.

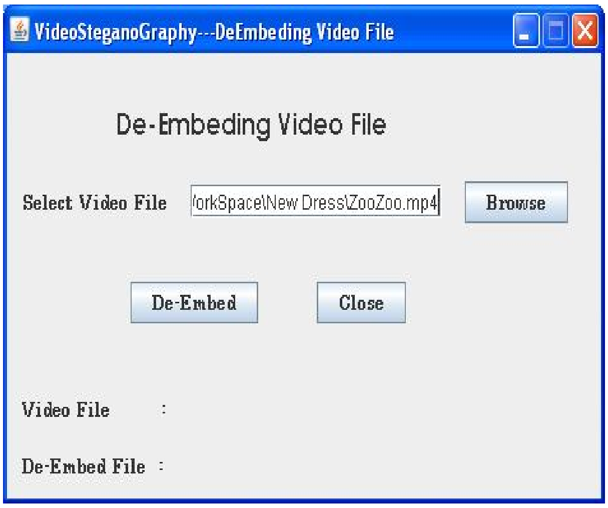


Select Encrypted File: \Key\Video Steganography\zoooooo
Select Video File: /orkSpace\New Dress\ZooZoo.mp4

Encrypted File : zoooooo
Video File :
Embeded File :

Figure 3 Illustrates embedding encrypted file into a video for secret sharing

As can be seen in Figure 3, the user interface allows the selection of video and encrypted files and the let the encrypted file to be embedded into the video file. Thus the video file when sent to a receiver which carries secret information that can be made to receiver only through the proposed key management scheme.



Select Video File: /orkSpace\New Dress\ZooZoo.mp4

Video File :
De-Embed File :

Figure 4 Illustrates de-embedding encrypted file from a video for secret information sharing

As can be seen in Figure 3, the user interface allows the selection of video file and the let the encrypted file to be extracted from the video file. Thus the receiver gets secret information only through the proposed key management scheme.

5. SIMULATION RESULTS

We have built a custom simulator in Java programming language to simulate WSN. The experiments are made to apply the proposed scheme in terms of efficient key management and also energy efficiency. Afterwards, our scheme is compared with the scheme presented in [17] where AVL tree is used for dynamic key update. This tree is a self-balanced binary tree which is efficient to update keys in real time. In this paper also we used AVL tree along with the new scheme we proposed. Our schemes security results are as presented in Table 2.

Table 2: Security of Proposed Scheme

Attack Type	Existing Scheme [17]	Our Scheme
Sybil Attack	YES	YES
Replication Attack	NO	NO
Replay Attack	NO	NO
Sink-Hole Attack	YES	YES
Selective Forwarding	YES	YES

As can be seen in Table 1, our scheme is able to prevent many attacks in WSN. We also made experiments with energy efficiency and compared with the methods of Yi-ying scheme, Tseng scheme, Cheikhrouhou scheme

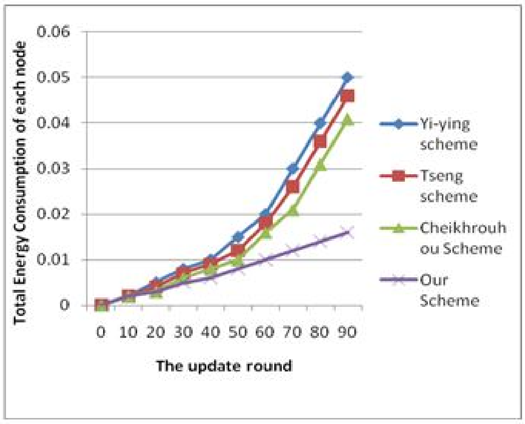


Figure 5 the Energy Efficiency of Nodes

As shown in Figure 5, it is evident that the energy efficiency varies among the schemes employed on WSN. Our scheme is showing better energy – efficiency performance when compared with other existing schemes.

6. Conclusion and Future work

In this paper we explored various key management schemes which provide security in Wireless Sensor Networks. As these wireless sensor networks are widely used in the real world environment, security plays a major role. These networks are vulnerable to attacks due to their resource constrained and mobility nature. Importance is to be given for secure communication among the nodes in the network. Key management and key distribution plays a pivotal role in providing secure communication. Many schemes came into existence but many of them are static in nature. They cannot provide their services to dynamic WSNs. In this paper we proposed a new key distribution scheme which makes secure communications over WSN. We built a prototype application to apply the proposed scheme for secret information sharing in the form of steganography. Our future work focuses on proposing a new key management scheme for secure routing in Dynamic Wireless Sensor Networks and its performance analysis.

References

[1] 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).

[2] A. Perrig, R. Szewczyk, J. Tygar, Victorwen and D. E. Culler, “Spins: Security Protocols for Sensor Networks”, ACM Wireless Networking, (2002) September.

[3] 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.

[4] 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.

[5] J. Zhang, Y. Sun and L. Liu, “NPKPS: A novel pairwise 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.

[6] L.Girod, T.Stathopoulos, N. Ramanathan, et al., “A System for Simulation, Emulation, and Deployment of Heterogeneous Sensor Networks”, Proc. of ACM SenSys, (2004).

[7] 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.

[8] 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.

[9] 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.

[10] 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.

[11] 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.

[12] 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.

[13] 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.

[14] 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.

[15] 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.

[16] 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).

[17] Y. -Y. Zhang, W. -C. Yang, K. -B. Kim and M. -S. Park, “An AVL Tree-Based Dynamic Key Management in Hierarchical Wireless Sensor Network”, International Conference on Intelligent Information Hiding and Multimedia Signal Processing, (2008).

AUTHORS

Dr. C. KrishnaPriya received her Master of Computer Applications from Sri Krishnadevaraya University, Anantapuramu, A.P., India, in 2007, M.Tech (IT) from KSOU, Mysore, Karnataka in 2011.She did her Ph.D in Computer Networks in the Department of Computer Science and Technology from Sri Krishnadevaraya University, Anantapuramu, A.P., India. Her current research interest includes Computer Networks, Network Security and Intrusion Detection.

Dr. P. Sumalatha received her M.Sc(Computer Science) from Sri Krishnadevaraya University, Anantapuramu, A.P., India, in 2007..She did her Ph.D in Computer Networks in the Department of Computer Science and Technology from Sri Krishnadevaraya University, Anantapuramu, A.P., India. Her current research interest includes Computer Networks, Network Security.