Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X
IMPACT FACTOR: 5.258

IJCSMC, Vol. 5, Issue. 4, April 2016, pg.384 – 390

Attack Resilient Dynamic Key Management for Dynamic Wireless Sensor Networks

RakeshReddy Gurrala[1], Pratibha Gaddampally[2]
Information Technology & Jawaharlal Nehru Technological University Hyderabad, India
Computer Science and Engineering & Jawaharlal Nehru Technological University Hyderabad, India
[1] rrgurrala@yahoo.com; [2] pratibhareddy19@gmail.com

Abstract--- Wireless Sensor Networks (WSNs) are widely used in both civilian and military environments. WSNs are vulnerable to attacks due to node mobility and resource constrained nature. However, the communications in WSN might be sensitive and need to be protected from malicious attacks. Traditionally cryptographic primitives are used for securing communications in WSN. However, the cryptographic methods used for wired networks may not be suitable for their wireless counterparts directly. In this paper we proposed a protocol that takes care of secure communications in WSN. The protocol is dynamic in nature. It supports dynamic key update so as to ensure that the old keys do not be able to compromise security of the network. The scheme also supports key revocation thus minimizing the impact of compromised nodes in the network. The scheme is evaluated with NS2 simulations and the results reveal that the proposed scheme is effective in securing communications in WSN.

Index Terms – ***Wireless sensor network, security, dynamic key management, key update***

I. INTRODUCTION

Wireless Sensor Networks (WSNs) became popular and used in different applications. For instance, it is used for monitoring patients, monitoring buildings, monitoring environments, surveillance and so on. In all such applications, securing communications is very important for many reasons. Many security schemes came into existence. They are based on cryptography with either asymmetric or symmetric nature. In this paper we proposed and implement a new scheme that takes care of secure communications with dynamic key management, key update, and key revocation in a dynamic WSN. The WSN we considered is heterogeneous in nature as presented in Figure 1. The sensor nodes are grouped into clusters. Each cluster has a cluster head which has specific responsibilities. The node which has high energy sources is elected as cluster head (CH). Cluster Node (CN) is responsible to sense data and sends to base station (BS).

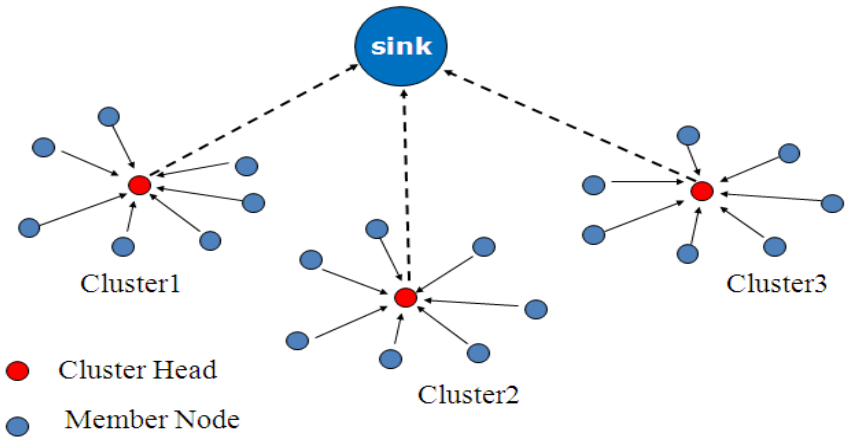

Figure 1 – Heterogeneous WSN

The sink shown in Figure 1 is also known as base station. It receives data from multiple clusters. The cluster heads only communicate with the base station. The sensor nodes in cluster communicate with cluster head. In this context, we proposed and implemented a dynamic key management scheme that takes care of secure key distribution, key update and key revocation.

A key management scheme with two layers was explored in [8] where dynamic key update protocol ensures the key change from time to time in order to provide high level of security to WSN. Similar kind of work was carried out in [7] as well. However, these two schemes fail when three are limited resources and the WSN is well known for its resource constrained nature. More details are in the ensuing sections. The remainder of the paper is structured as follows. Section II provides review of literature. Section III provides details of the proposed scheme. Section IV presents the experimental results while section V concludes the paper.

II. RELATED WORKS

Key management is very important in WSN. There key management schemes can be classified into two categories. They are symmetric and asymmetric. This section provides review of literature on dynamic key management schemes employed in WSN. A key management scheme with two layers was explored in [1] where dynamic key update protocol ensures the key change from time to time in order to provide high level of security to WSN. Similar kind of work was carried out in [2] as well. However, these two schemes fail when three are limited resources and the WSN is well known for its resource constrained nature. Therefore it is challenging to make use of such WSN for securing applications in the real world. Identity based PKC and other schemes came into existence. Especially ID based PKC schemes explored in [3] and [4] in which experiments were made and concluded that there were not efficient as they cause computational overhead for pairing operations that are mandatory for security of WSN.

A certificate less key management scheme is proposed in this paper. There are many certificate oriented schemes such as [5] where KGC is required in order to generate secret values. The benefit of ECC keys was considered along with secure RSA scheme with 1024 bit length used for security mechanisms. The security primitives are based on the random oracles instead of standard implementations. Many ECC based schemes came into existences as explored in [6], [7], and [8]. ECDSA is a scheme [6] which can verify the identity of cluster head in a heterogeneous network.

According to the explorations provided in [9] and [10], it is essential that a dynamic key management scheme should have certain security properties as described here. Compromise –reconcile is an important attribute that ensures that even a node is compromised, the network should not fail to function normally. Even when a node is captured by hackers, the network should continue functioning well. Impersonation is another important attribute for security. It does mean that there should be provision to cope with impersonation in which a node acts as another node illegally. Forward and backward secrecy is essential in order to have compatibility so as to prevent nodes from using old identities and keys in order to ensure high level of security. These are bet used for avoiding node-capture attacks.

III. PROPOSED SCHEME

The proposed scheme is meant for protecting WSN from malicious attacks. The network is secured using the proposed scheme which takes care of initialization, secure key distribution, key update and key revocation.

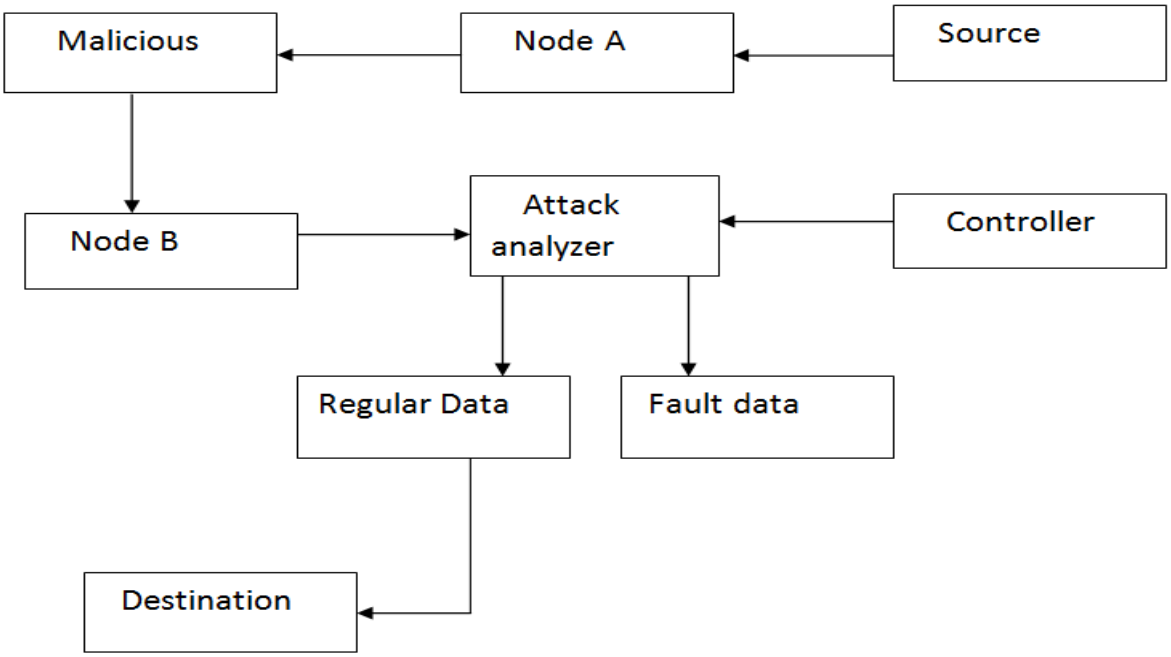

Figure 2 – Overview of the proposed scheme

As shown in Figure 2, we implemented attack analyzer which takes care of security issues besides ensuring that the communications in the network are protected from malicious attacks. The controller sensor nodes and the attack analyzer work in tandem with each other in order to prevent attacks and promote secure communications.

IV. EXPERIMENTAL RESULTS

Simulations are made in NS2 for proof of concept. WSN is built with many sensor nodes and a base station. There is attack analyzer which takes care of attacks and prevents them. The scheme is employed in the network in order to have secure communications.

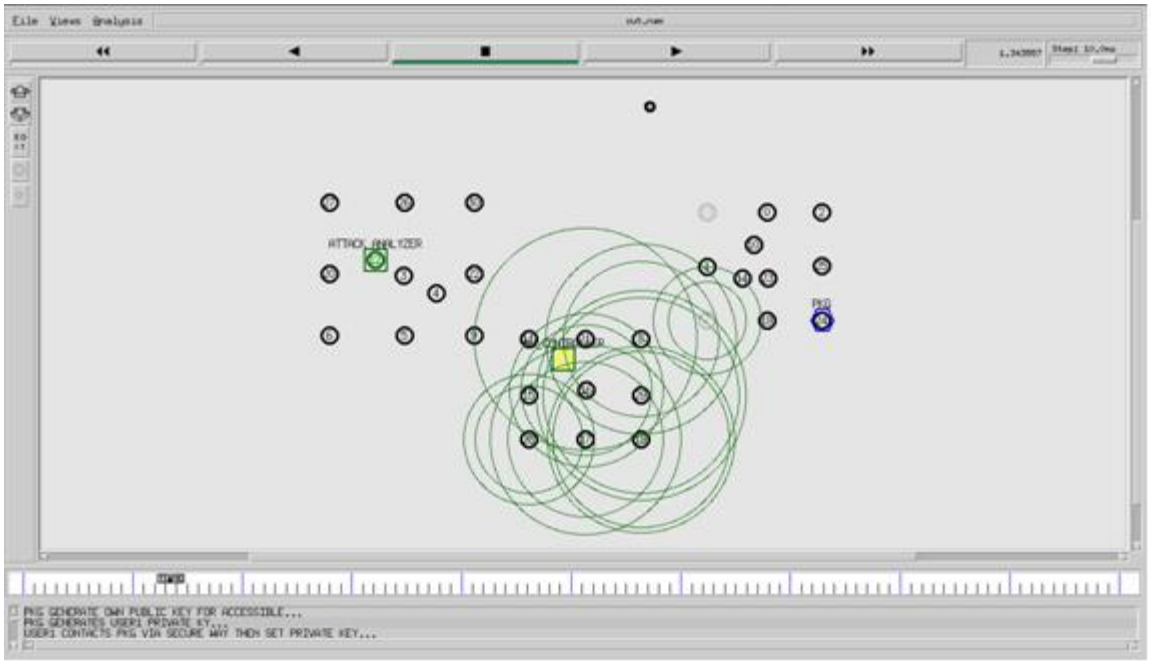

Figure 3 – Simulation of WSN showing protocol propagation

As can be seen in Figure 3, the protocol propagation is simulated with different sensor nodes, base station and attack analyzer.

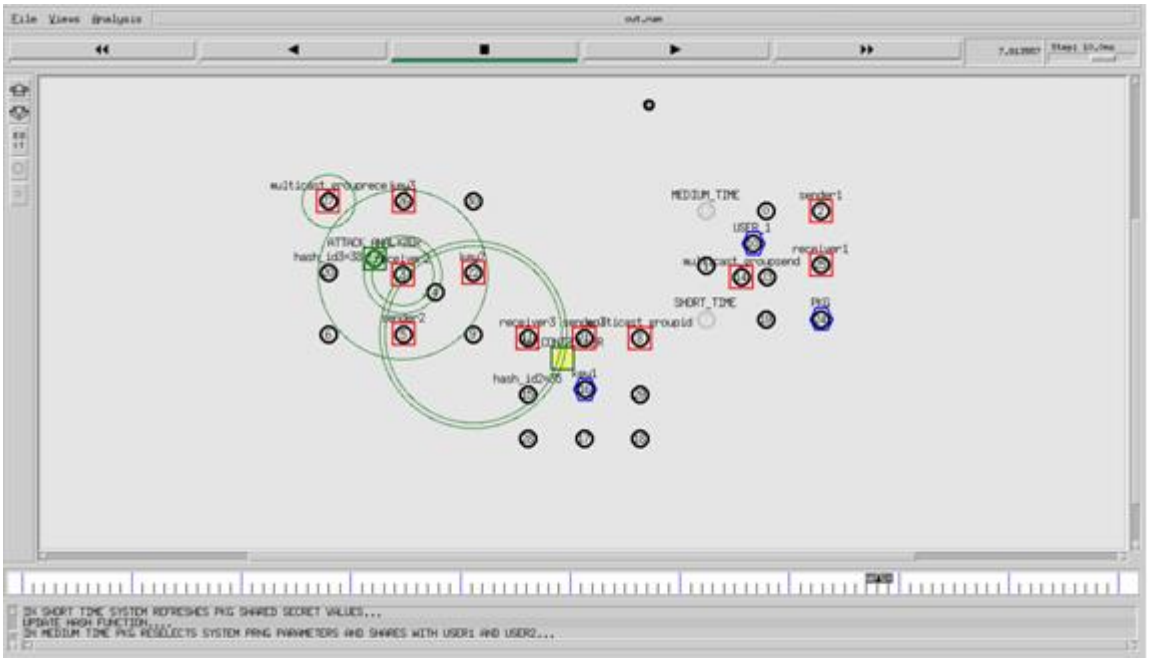

Figure 4 – Simulation of WSN showing PKG sharing secret keys

As shown in Figure 4, it is evident that the simulation reveals the PKG generating keys and sharing to nodes in the network. It also shows the sender and receiver nodes and the functioning of attack analyzer.

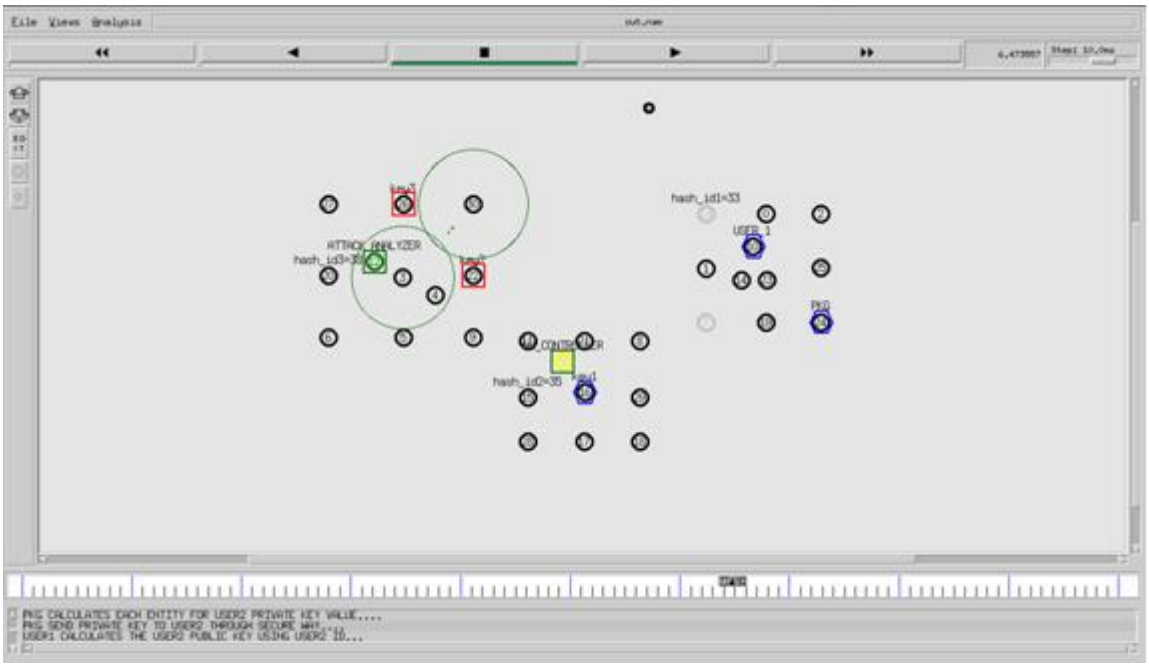

Figure 5 – Secure communication between nodes

As shown in Figure 5, there is secure communication established among the nodes of WSN. The attack analyzer is able to perform its duties in order to have secure communications in the WSN.

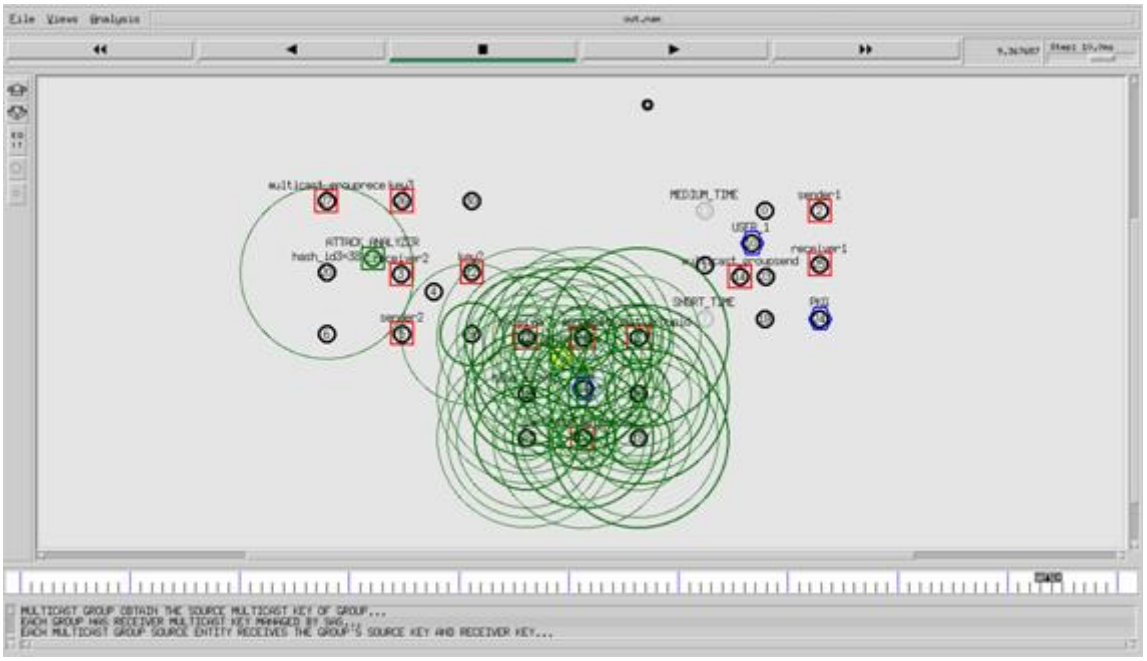

Figure 6 – Secure communication and prevention of attacks

As can be seen in Figure 6, it is evident that the secure communication and prevention of attacks is made possible with attack analyzer protecting communications between nodes and the base station.

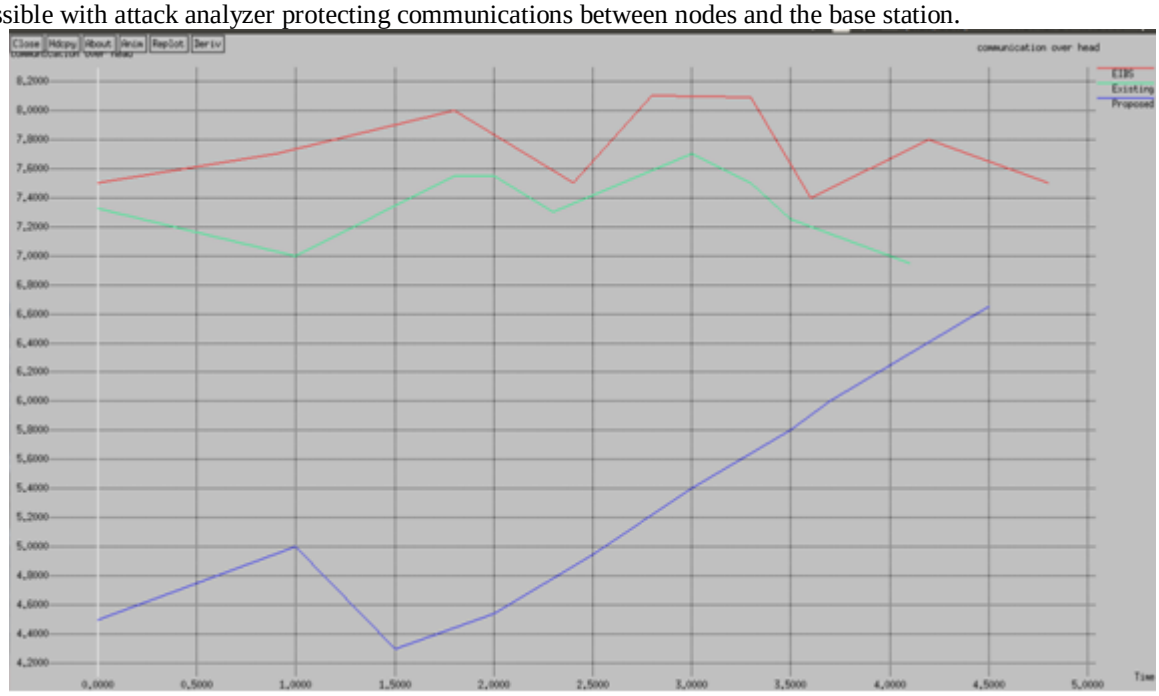

Figure 7 – Comparison of communication overhead

As can be seen in Figure 7, it is evident that the communication overhead of the proposed system is compared with existing systems. The results revealed that the proposed system outperforms the existing systems.

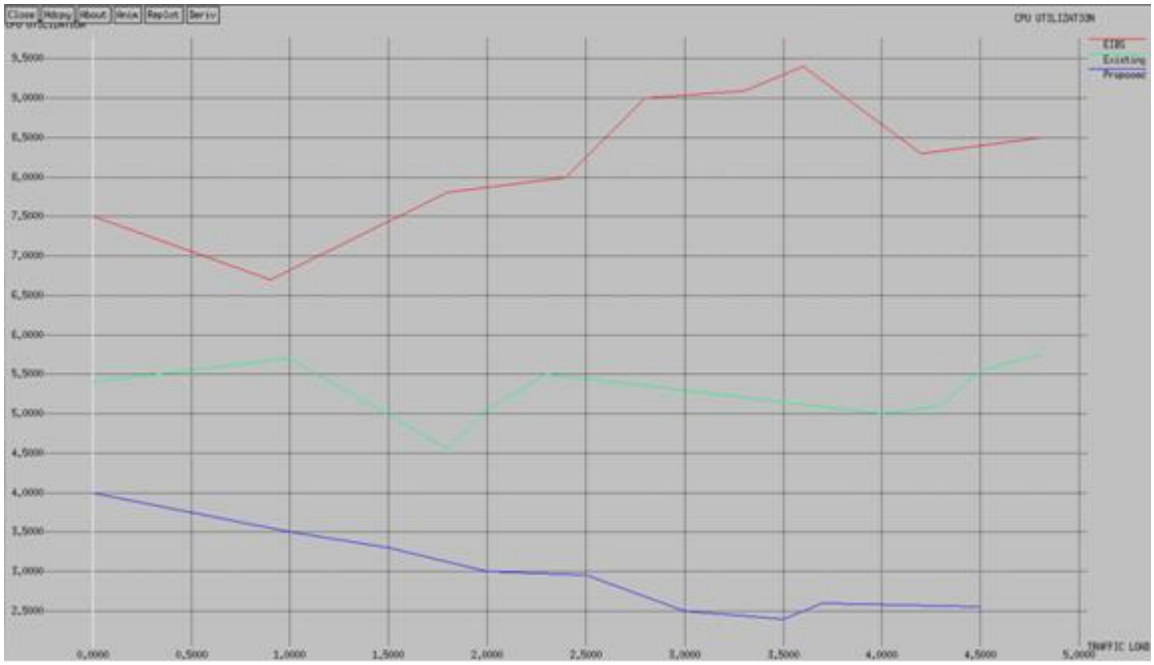

Figure 8 – Comparison of CPU utilization

As can be seen in Figure 8, it is evident that the CPU utilization of the proposed system is compared with existing systems. The results revealed that the proposed system outperforms the existing systems.

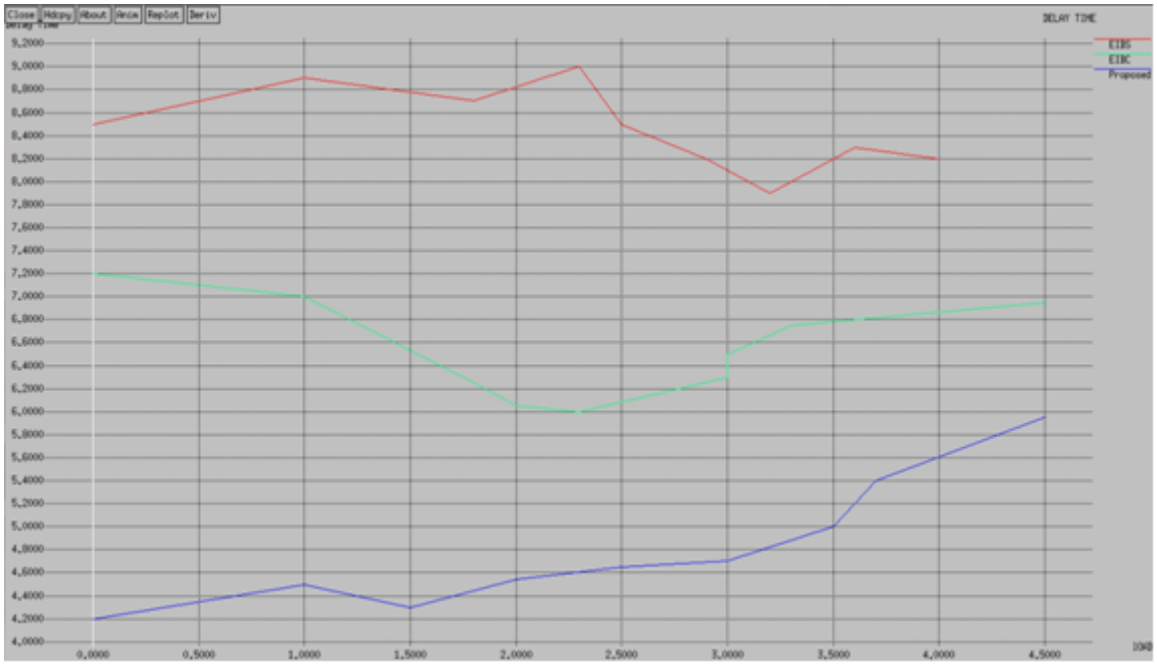

Figure 9 – Comparison of delay time

As can be seen in Figure 9, it is evident that the delay performance of the proposed system is compared with existing systems. The results revealed that the proposed system outperforms the existing systems.

V. CONCLUSIONS AND FUTURE WORK

In this paper we studied the WSNs in the context of dynamic key management. We found in the literature most of the schemes are either using dynamic WSN or dynamic key management. In this paper we propose and implement a novel key management scheme which is dynamic in nature and works for dynamic WSN. The scheme has provision for key establishment, key distribution, key update and key revocation. Thus it can handle compromised nodes using key revocation approach. The proposed scheme is implemented in NS2 and the simulations reveal that the scheme is useful for protecting communications in WSN besides making the network

as attack resilient. This research can be extended further to explore different kinds of attacks explicitly in order to make it resilient and robust to different kinds of attacks.

REFERENCES

[1] S. Agrawal, R. Roman, M. L. Das, A. Mathuria, and J. Lopez, "A novel key update protocol in mobile sensor networks," in Proc. 8th Int. Conf. ICISS, vol. 7671. 2012, pp. 194–207.
[2] I.-H. Chuang, W.-T. Su, C.-Y. Wu, J.-P. Hsu, and Y.-H. Kuo, "Twolayered dynamic key management in mobile and long-lived clusterbased wireless sensor networks," in Proc. IEEE WCNC, Mar. 2007, pp. 4145–4150.
[3] K. Chatterjee, A. De, and D. Gupta, "An improved ID-based key management scheme in wireless sensor network," in Proc. 3rd Int. Conf. ICSI, vol. 7332. 2012, pp. 351–359.
[4] M. Rahman and K. El-Khatib, "Private key agreement and secure communication for heterogeneous sensor networks," J. Parallel Distrib. Comput., vol. 70, no. 8, pp. 858–870, 2010.
[5] S. S. Al-Riyami and K. G. Paterson, "Certificateless public key cryptography," in Proc. 9th Int. Conf. ASIACRYPT, vol. 2894. 2013, pp. 452–473.
[6] D. Du, H. Xiong, and H. Wang, "An efficient key management scheme for wireless sensor networks," Int. J. Distrib. Sensor Netw., vol. 2012, Sep. 2012, Art. ID 406254.
[7] X. Zhang, J. He, and Q. Wei, "EDDK: Energy-efficient distributed deterministic key management for wireless sensor networks," EURASIP J. Wireless Commun. Netw., vol. 2011, pp. 1–11, Jan. 2011.
[8] M. R. Alagheband and M. R. Aref, "Dynamic and secure key management model for hierarchical heterogeneous sensor networks," IET Inf. Secur., vol. 6, no. 4, pp. 271–280, Dec. 2012.
[9]H. Chan, A. Perrig, and D. Song, "Random key predistribution schemes for sensor networks," in Proc. IEEE Symp. SP, May 2003, pp. 197–213.
[10] X. He, M. Niedermeier, and H. de Meer, "Dynamic key management in wireless sensor networks: A survey," J. Netw. Comput. Appl., vol. 36, no. 2, pp. 611–622, 2013.

AUTHORS

Mr.Rakeshreddy Gurrala, working as Assistant Professor in the Department of Information Technology at Keshav Memorial Institute Of Technology (KMIT), Hyderabad. I did my M.Tech in Information *Technology* from JNTUH and B.Tech in Information Technology from JNTUH. My research interests network security and wireless sensor networks and mobile computing.

Ms.G.Pratibha is working as Assistant Professor in the Department of *Computer Science and Engineering* at Matru Sri Engineering College (MECS), Hyderabad. I am pursuing Ph.D at JNTUH Hyderabad. I had 10 years of teaching and 4 years of research experience. I published 7 International Journals and attended 4 International/National Conferences. My research interests **NLP, Data Mining, Automata, Compiler Design**

