A Paired Key Mechanism for Wireless Link Security for WSNs

Gagandeep Kaur, Navjot Kaur
Mtech Student, Assistant professor
Computer Science & Enggineering,Kharar, India

***Abstract* - The wireless sensor network has been used in many applications for military, weather, industrial or many other industries. The wireless sensor networks are consisted of the low configuration nodes with limited battery life. The security issues have been raised as one of the major concerns for the sensor networks. The security solution designed for the sensor nodes must be capable of mitigating the attacks with the minimum energy consumption and it should not hurt the performance of the sensor networks at all. In this paper, a quick encryption method with lightweight key management scheme has been proposed for the purpose of security mechanisms of authentication for the sensor networks. The proposed model has been designed to provide the best level security by using the lightweight randomized keys form the 2-column table as the maximum possible energy efficient approach. The proposed model results have been evaluated against the existing models and it has been found effective on the basis of all of all of the obtained parameters. The experimental results have marked the proposed model results as better than the existing model.**

***Keywords* - Key management, lightweight key scheme, crypto key management, AKA, CBC.**

I. INTRODUCTION

Wireless sensor network mainly consists of huge number of autonomous devices, which are battery-powered and each device is known as sensor node. These sensor nodes are dispersed over a particular area and are capable to gather and transmit information about the environment as to provide fine explanations of a phenomenon. A sensor node is equipped with one or more sensors, data processing capabilities, short-range radio communications, a small amount of memory and a power supply. Sensor devices work together which each other in order to perform basic operations for example sensing, communication and data processing.

Due to increase in movable devices in wireless communication, wireless sensor networking applications have become widespread. Major applications using WSNs include monitoring and tracking. These applications are used in different areas like environmental monitoring, area monitoring, health care monitoring, entertainment purposes, emergency services, military battlefield, industrial monitoring. These sensor networks provide security at various places like at supermarkets, homes, agricultural fields and also, monitors the vehicle traffic on main roads, railways, oceans, sea etcetera. Environmental monitoring helps biologists study sensitive wildlife habitats, for example the micro-climates on Great Duck Island, Maine. Health care applications do constant monitoring of patient's health through sensors. In military, sensors are used for controlling, computing, reconnaissance, intelligence, battlefield surveillance and targeting systems and sensing the presence of enemies, dangerous equipments like poisonous gases and explosions.

There is an increasing interest in the field of wireless sensor networks due to the recent advancements in wireless communication and microelectronics. A sensor network includes conveying a variety of sensors for distributed monitoring of real time events. As the sensor nodes are battery powered, the sensor networks have limited energy. Also, small amount of memory and computational capability is held in sensor nodes and can be deployed in remote areas. These sensor networks are used for different life critical applications such as monitoring patients in hospitals and military applications. So to use sensor networks in these applications, a good security infrastructure is essential. It is very challenging issue to make design of security protocol due to the limited power and memory. In this paper security issues in Directed diffusion are addressed. Directed Diffusion is a novel routing protocol for sensor networks. A look-in to possible attacks and counter measures is provided. The paper is concluded with a brief analysis on the possible countermeasures to prevent such attacks.

The security of Wireless Sensor Networks(WSN) can be compromised in many ways. A remote end user accessing base station information can be prevented from doing so in a variety of ways. Communication between the base station and sensor nodes can be blocked. This can be accomplished by analog jamming of signals or by digital jamming in the form of DoS(Denial of Service) attacks that flood the network, base stations or both. Targeted DoS attacks on strategic nodes in the WSN can also block communication of large parts of the network with the base station. Communication between base stations and other sensor nodes can be prevented by setting up incorrect routing information so that traffic goes to the wrong destination or loops. One way to do this is to spoof the base station and deceive nodes into rerouting all packets to the spoofed base station instead of the real base station.

Another way of breaching security is to destroy the base station itself. This can be accomplished by monitoring the volume and direction of packet traffic toward the base station so that the location is eventually revealed. Destruction can also be accomplished by listening to the RF signals to localize and triangulate the location of the base station. A third threat is eavesdropping. This is made easier by wireless hop-to-hop communication. Eavesdropping can be used to track and deduce the location of the base station for destruction. There are many other methods to breach the WSN security. These attacks are usually

caused because of the lack of security in the sensor node inter communications. For instance, a hacker can easily make a connection with the insecure wireless sensor nodes to infect or jam the whole sensor network. These types of attacks can be reduced or stopped by use of proper key management schemes in the entire network to provide secure communication as the efficient key management techniques exchange the secure cryptographic keys between the nodes.

During the periods when the WSN nodes are in working condition, they need secure cryptographic keys for secure propagation of the sensitive information. Efficient key management and distribution scheme play an important role for the data security in WSNs. Existing cryptographic key management and distribution technique usually consume higher amount of energy and put larger computational overheads on Wireless Sensor Nodes. The cryptographic keys are used on different communication levels of WSN communications i.e. neighbor nodes, cluster heads and base stations. An effective corporate key management and distribution policy is required to maintain the security of the wireless sensor networks.

II. LITERATURE SURVEY

Prasad et.al (2011) observed that security is an essential part in WSN and it is compulsory to preserve secrecy and privacy of transmitted data. So, a reliable security model (RSM) was presented for WSNs. In that model, four keys were used from which two were static and two were dynamic. From two static keys, one key was attained by composition of Q number of keys and other one was real-time MACID. While calculated dynamic keys randomly and each time when network was resynchronized, these keys were changed. In reliable security model, time taken by an invader more than total time of synchronization, so even if the node got compromised, the value of key had already been changed. Also, RSM provided large amount of energy to the Base station and to the sensor networks. As that way, continuous serving of data occurred instead of interrupted sensing of data by providing high energy to BS. **Alagheband and Aref (2012)** proposed a dynamic key management infrastructure for the mixed WSNs which were based on elliptic curve cryptography and between the clusters and base stations with the help of signcryption technique instead of doing encryption with signature, sensor node versatility, verification to save sensor node traded off in the clusters. The proposed plan had system versatility and sensor node portability particularly in fluid situations. Both occasional verification and another enrollment mechanism were proposed through counteractive action of sensor node traded off. The creators investigated a portion of more influential varied WSN key administration plans and contrasted them with the proposed plan. After contrasting the proposed plan with more determined progressed mixed WSN key management conspires, the proposed system separately turned out to be better as far as correspondence, calculation and key storage. The scheme was proposed after observing the various types of insecurities among the wireless sensor network.

He et.al (2013) presented a diagram of cutting edge dynamic key administration conspires in WSNs. With the wide utilization of WSNs, as one of the basic security issues, element key administration was drawing in more consideration from the analysts and industrial specialists and numerous plans were at that point proposed. They examined the essential necessities of element key administration in WSNs, studied the proposed plans for those situations and highlighted the security and execution favorable circumstances and weaknesses of every plan. At long last, outlined and broke down those systems as indicated by the discussed assessment measurements. In rundown, it was impractical to locate one single perfect plan to perform well in all assessment measurements as each of them had some positive qualities, shortcomings and suitability for particular circumstances. A definitive goal of that study was to urge more analysts to outline and enhance potential recommendations in dynamic key administration for remote sensor systems. **Zhou et.al (2013)** proposed a Key management algorithm named as Key it Simple and Secure (KISS) to enable comprehensive, trustworthy, user-verifiable, and cost-effective key management. KISS protects the entire life cycle of cryptographic keys. In particular, KISS allows only authorized applications and/or users to use the keys. Using simple devices, administrators can remotely issue authenticated commands to KISS and verify system output. KISS leverages readily available commodity hardware and trusted computing primitives to design system bootstrap protocols and management mechanisms, which protects the system from malware attacks and insider attacks.

Abdallah et.al (2014) proposed an elliptic curve public key cryptography based key management scheme that ensured secure sharing of many types of keys in each level of the network topology. Particularly, it used elliptic curve Diffie-Hellman like key exchange procedure to establish pair wise keys between the sensor node, the base station, and its cluster head. Also, a group key establishment protocol was proposed to create a cluster key used to secure communication within each cluster and an inter-cluster key used to secure message exchange between the cluster heads and the base station. Those keys enabled in-network processing, which improved message transmission efficiency and resources usage in the WSN. Furthermore, they also enabled re-keying procedure based on the concept of threshold secret sharing mechanism. **Bellazreg and Boudriga (2014)** proposed Dynamic Tunneling & group Key Management Protocol (DynTunKey) which was a secure novel group key protocol for WSN and examined the use of secure tunnels to recover the protection of WSNs. That protocol created dynamic tunnels in between the sensor nodes. Firstly to get the formation of tunnels, protocol maintained shared cluster security technique among SNs that were able to discover the same result. After that, a solution was proposed so that dynamic integration could be done in secured communication channel. Also, number of tests had been carried out to calculate the efficiency of newly proposed technique in regard to topical key management protocols and to old key management protocols that were built using IPSec protocols. The protocol had various benefits as it decreased the computational overhead reducing the number of transmitted data. The DynTunKey protocol was tested with two models of mobility from which one was Random Walk model and another was the Gauss Markov model.

Kodali and Kishore (2014) proposed a combination of symmetric and asymmetric key primitives at different levels of hierarchy as to minimize the energy overhead. The communication and computational operations consume most of the energy, when security protocols are applied to resource constrained sensor nodes. To minimize these overheads and at the same time to provide the required security level, the resource consuming IBK technique was applied between cluster heads and the base station only.

The secure cluster formation and key reinforcement mechanisms applied in that scheme restrict the node capture attack and other network attacks to the cluster alone.

III. EXPERIMENTAL DESIGN

The proposed model has been designed as the robust crypto key based authentication scheme for the wireless sensor network. The proposed model has been designed to work during the data communication phase. The data communication phase can be defined as the phase, where the two nodes transfer the data between them while sending the data towards the sink node or the base station node. The proposed model has been designed to work in the lightweight paired` behavior over the secure communication link. The proposed model has been designed using the randomized for key table generation, which consumes the one-time resources and in-return produces the any size of rows in the key table. The keys in the table remain in the paired relationship which does not change during any stage in the session. The paired relationship model between the keys in the different columns saves the sensor networks from the external attacks. The paired relationship based key pairs are secured during the communication by encrypting the key data. The paired relationship based key model with key encryption add the extra layer of security to the sensor networks to prevent the passive attacks like replay attack, replication attack or the sniffing attacks. Also, the proposed model can prevent the active attacks by preventing the connections from the unauthorized sensor or attacker nodes. The proposed model algorithm is as following:

Algorithm 1: Paired Key Mechanism (PKM) Algorithm

1. The sensor nodes start up and begin the information broadcasting in the cluster.
2. The sensor node send the open connection request to the other nodes within the range
3. Within range sensor nodes reply with the connection request acceptance in the form of acknowledgement.
4. The sensor nodes runs key table generation module and generation key table Kt(i), where Kt is the key table and i defines the node id.
5. If initial level communication is successful and both side acknowledgements have been successfully shared, the nodes exchange the key table information with the neighbor nodes.
6. Once the path information setup complete, the nodes decide their point-to-point role, where one node becomes the server or sender and other receiver or client.
7. Whenever, the sender has some data for the receiver or next-hop node in the path towards the sink node, the sender node computes a key from the key table 1-column.
8. The keys is then encrypted and forwarded to the receiver end or client end.
9. The client decrypts and lookup the paired key in the key table and returns it to the sender or server node.
10. The sender node decrypts and computes the decision logic.
11. If the decision logic is returned true, the data transfer begins.
12. Otherwise the data is not sent and node lookup for the alternative secure path.

IV. RESULT ANALYSIS

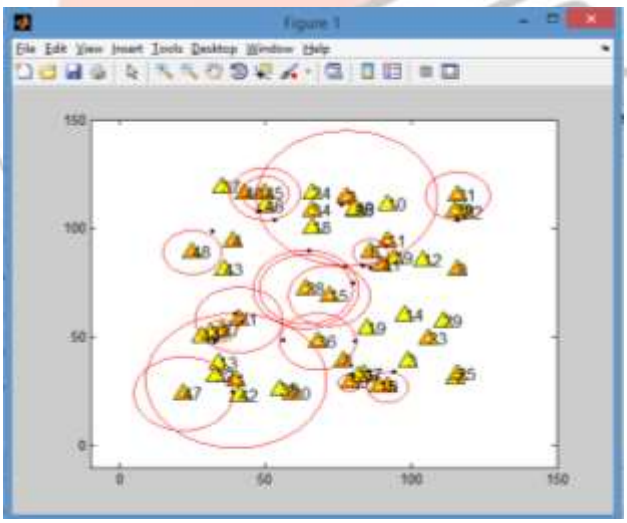

Figure 1: The WSN topology has been shown in the above figure.

The nodes have been deployed in the random function without the overlapping factor avoidance. The random deployment factor has been used to overcome the nearest covariance to the sensor topology.

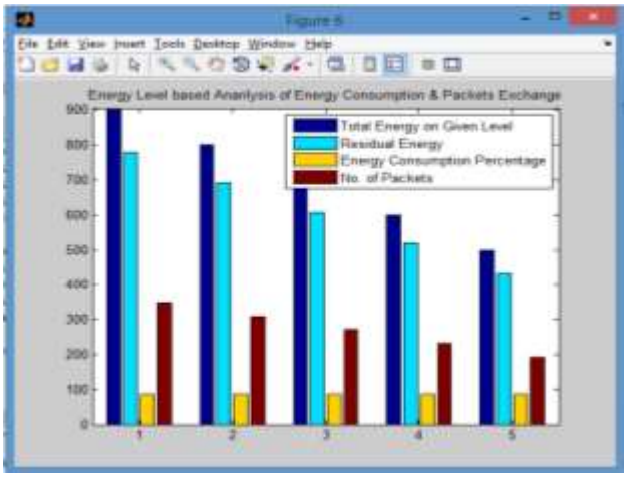

Figure 2: The energy consumption to number of packets ratio

Fig 2 shows the variation in the energy consumption on each energy level. The above figure has been obtained after assigning the energy levels to the sensor networks during the different levels of the simulation. Each level has been tested for the number of packets which can be transmitted while the energy is consumed upto the specific given level. The number of packets has been recorded along with the remaining energy level and the percentage of the energy consumed to transfer the packets for the given energy threshold. Lets say the initial energy levels is set to 100 and the threshold level is set to 40. Each packet consumes energy index of 1 for the data transmission or receive. The WSN topology is consisting of 3 nodes, where one node only sends the data, one only receives and one undergoes the intermediate node operation. One packet transmission consumes the energy index of 4. The energy level of 60 will transmit the 15 packets in the sensor network, which will leave the residual energy at 40, consumed energy percentage at 60 and 15 number of packets transferred.

V. TIME BASED ANALYSIS

The time taken for various procedures in the key exchange scheme has been recorded during the sensor communication in the proposed architecture simulation in the MATLAB simulator. The elapsed time has been recorded for various procedures: Time for Key generation, Time for key sharing or transfers, Time for key verification.

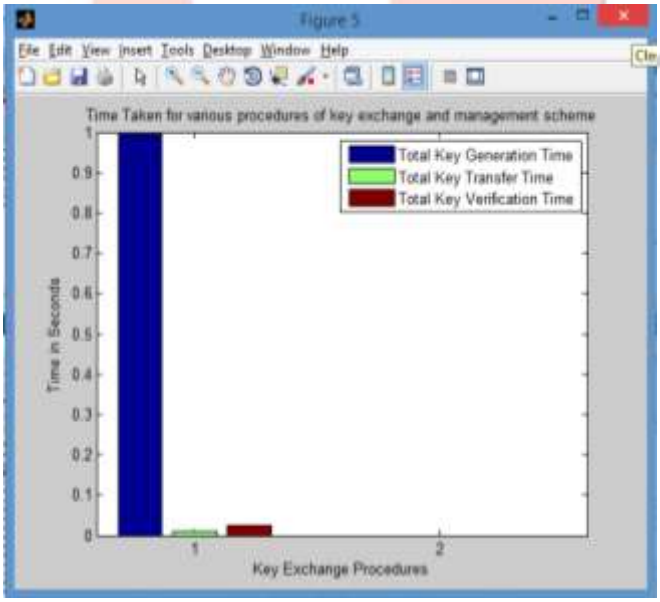

Figure 3: Bar Graph presentation of key generation, key transfer and verification schemes

The key scheme has been evaluated for the key generation time, key verification and key transfer times across the WSN cluster. The key generation time is the highest because the random factor calculation in the proposed model. The key generation is the one time process and taken approximately 1 second during the initial phase of the communication in the wireless sensor nodes. The key verification and key transfer times has been recorded in the averaging factor. The key verification and key transfer time are known to have taken less than 0.1 second for the completion of their process, which makes the whole system completely efficient.

Table 1: The time based analysis (Averaging factor)

Key Generation Time (One time process)	1 second
Key Transfer Time (Average)	0.01 seconds
Key Verification Time (Average)	0.02 seconds

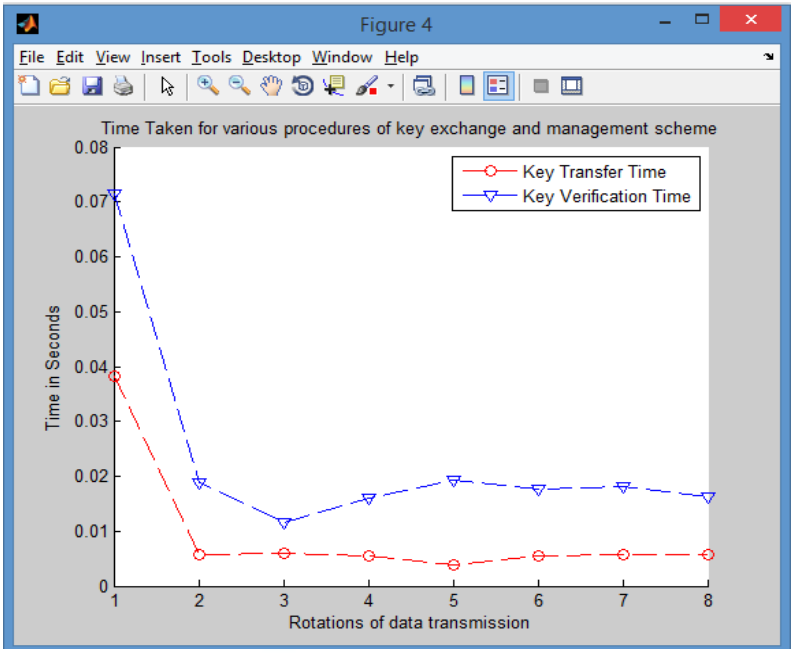

Figure 4: Line Graph presentation of key transfer and verification schemes

The above graph represents the key transfer time and key verification time recorded during the various key exchange intervals in the simulation. The key exchange interval has been set to 1 second in the simulation. It means the key is being exchanged every second between the two ends of the communication link in the sensor node network. The proposed model has been proved to be very efficient as it adds approximately 2/100th factor of communication overhead over the given WSN link, which is considered very low for a key exchange scheme. The Average time has been taken for key transfer time at 0.01 seconds and 0.02 seconds for the key verification time. The proposed model has taken the maximum of 0.07 seconds for the key verification where the lowest value remains at the 0.013 seconds, whereas the key verification time has been recorded lowest at 0.005 seconds and highest at 0.038 seconds.

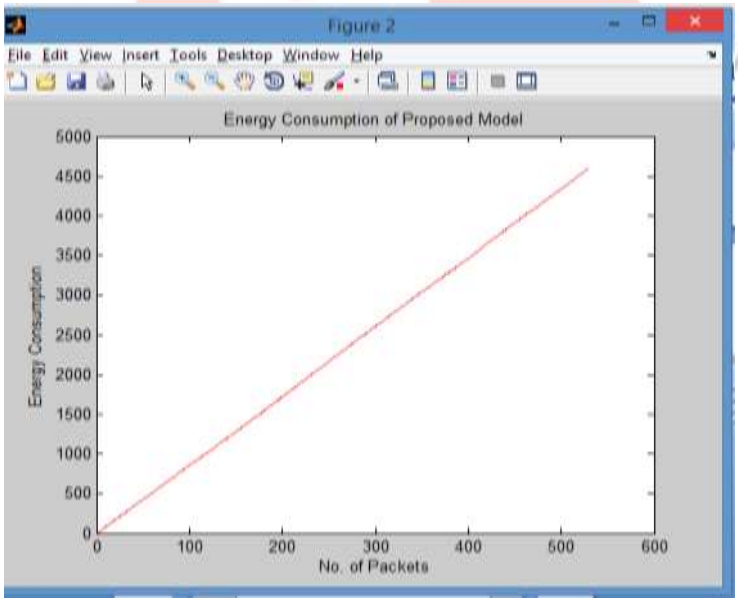

Figure 6: The energy consumption graph

The energy consumption graph has been recorded from the simulation environment. The key exchange overhead hasn't put any affect over the graph, and allows the graphs to become linear where a constant data is being sent over the communication links.

COMPARATIVE ANALYSIS

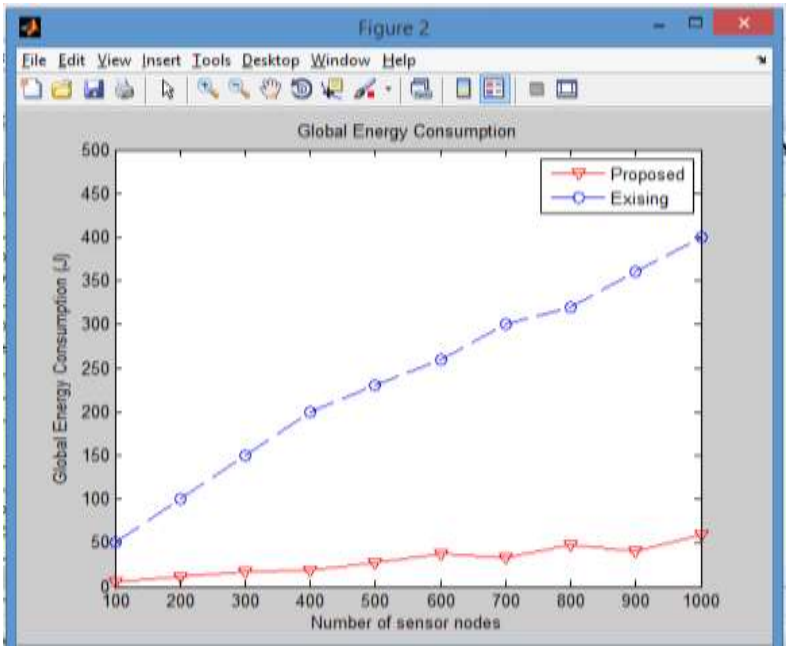

Figure 7: Global energy consumption based comparison of proposed and existing scheme.

The existing model has been compared to the proposed model on the basis of global energy consumption, where the proposed model has been proved to be efficient. The global energy consumption factor calculates the overall energy consumption in the whole sensor network in the form of average. The global energy consumption factor signifies the performance of the sensor network in delivery the packets efficiently while consuming the less amount of data. The proposed model has been proved to be efficient in the case of proposed model. The proposed model has been found almost 10 times efficient than the existing model. The proposed model energy consumption has been found between 1 and 60, where the existing model has been recorded as the way higher values between 50 and 400. This shows the concrete improvement in the performance of the proposed model in comparison with the existing model.

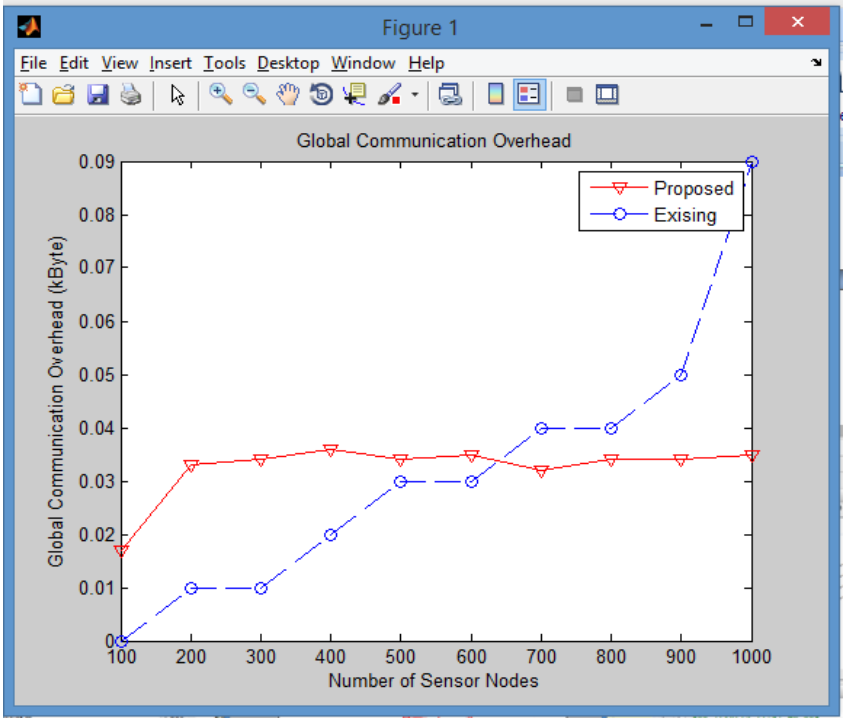

Figure 8: The global communication overhead based comparison of the existing and proposed model.

The proposed model performance has been evaluated in the form of the communication overhead and has been compared to the existing system. The communication overhead of the existing system varies between 0.01and 0.09 kBytes every second, whereas the proposed model has been recorded between the 0.017 to 0.034 kBytes every second. The proposed model has been performed much consistently, which shows the stability of the proposed model in adapting the higher number of nodes. The sensor network with higher number of nodes than 500 will be secured and made efficient by using the proposed model.

VI. CONCLUSION

The proposed model results have been evaluated on the basis of various performance parameters, such as energy, key management time, global communication overhead, etc. The proposed model has been tested under the different numbers of

nodes, from which the results of simulation topology with 50 nodes has been collected and analyzed thoroughly to define the performance level of the proposed model. The proposed model has been found performing better in the terms of energy consumption, KTG (key table generation) duration, elapsed time, etc. The experimental results have proved the effectiveness of the proposed, when compared to the existing models for the similar reason. The proposed model has been found resistant against the several forms of passive attacks with the data altercation intentions such as replay, replication or sniffing attacks. Also the proposed model resists the intruders from entering into the sensor network, which directly or indirectly provides the security against many forms of the active attacks.

VII. FUTURE WORK

In the future, the proposed model key management scheme can be enhanced with the double encryption scheme or other novel quick encryption model. The proposed model can be compared with other data communication security models using the key information exchange.

VIII. REFERNCES

[1] Abdallah W., Boudriga N., Kim D. and An S. (2014) *"An efficient and scalable key management for Wireless Sensor Networks"* in Advanced Communication Technology (ICACT),2014 16th international conference on IEEE, pp. 687-692.

[2] Alagheband M.R. and Aref M.R. (2012) *"Dynamic and Secure Key Management Model for Hierarchical Heterogeneous Sensor Networks"* Institution of Engineering & Technology Information Security, volume 6, issue 4, pp. 271-280.

[3] Bellazreg R. and Boudriga N. (2014) *"DynTunKey: A Dynamic Distributed Group Key Tunneling Management Protocol for Heterogeneous Wireless Sensor Networks"* EURASIP Springer International Publishing Journal on Wireless Communications and Networking, pp. 1-19.

[4] He X., Niedermeier M. and Meer H. (2013) *"Dynamic Key Management in Wireless Sensor Networks: A Survey"* Journal of Network and Computer Applications, volume 36, issue 2, pp. 611-622.

[5] Kodali R.K. (2014) *"Key Management Technique for Wireless Sensor Networks"* Region 10 Symposium, 2014 IEEE, pp. 540-545.

[6] Prasad D., Gupta M. and Patel R.B. (2011) *"A Reliable Security Model Irrespective of Energy constraints in Wireless Sensor Networks"* International Journal of Advanced Computer Science and Applications, volume 2, issue 4, pp. 20-29.

[7] Zhou Z., Han J., Lin Y.-H., Perrig A. and Gligor V. (2013) *"KISS: Key It Simple and Secure corporate Key Management"* Trust and Trustworthy Computing Lecture Notes in Computer Science, volume 7904, pp. 1-18.