IJCTA, 9(12), 2016, pp. 5815-5825
© International Science Press

Securing Data Transactions in Wireless Sensor Networks using a Certificateless Key Management Systemized Environment

***N. Tharminie **N.Durai Pandian**

Abstract : In recent times, WSNs (wireless sensor networks) have come to be used in key applications in military surveillance, healthcare and environmental sciences. The business of secure data and communications needs proper encryption key protocols, and in order to accomplish safer communications CL- EKM is of paramount significance in dynamic WSNs. CL-EKM continues to maintain effective communications for latest information and administration whenever a node departs or connect a cluster and, therefore, guarantees onward and backward key confidentiality. The suggested mechanism is based on CL-EKM with factors relating to movement of nodes. This method can be used to evaluate the correct assessment for the Thold and Tback . The factors are based on the required transaction flanked by energy consumption and security levels and the velocity. The suggested method is flexible against compromised nodes, cloning and impersonation attacks, in addition to safeguarding data secrecy and integrity. The outcome testifies the efûciency of CL-EKM in resource-limited WSNs, with the NS2 simulator used to implement this efficient method. The upcoming work aims at the possibility of using SET-IBS and SET-IBOOS protocols with regard to security needs and analyzing the outcomes against different attacks, since the main shortage of symmetric key management for protected data transmission is safe and competent data transmission protocols.

Keywords : Certificateless Effective Key Management, Efficient Data Transmission Protocols, Secure Data Transmission, Wireless Sensor Networks.

1. INTRODUCTION

Physical factors such as light, temperature, humidity and vibrations are managed by a WSN made up of a huge array of sensor nodes extended over different geographical areas. WSNs are extensively used in sundry critical applications. Communication between two nodes mandates utmost security, given that sensor nodes are prone to security attacks. Fig.1 shows a model design of a wireless sensor network. WSNs are networks of small, independent nodes fitted with wireless transmission and sensing capabilities for a large variety of applications like healthcare, transportation, industrial manufacturing automation and smart grids.

Data is collated by sensor nodes and thereafter transmitted to the base station to be processed, following which it reaches the user through a wireless medium. WSNs are utilized in umpteen applications such as enhancing output, maintenance of monitoring systems, and improving security and safety. However, for extensive deployment of WSNs, it is necessary that sensors be low-cost, made smaller and the network protected from attacks by means of certain techniques currently being proposed. Fig 1 shows the architecture of WSN fields. Sensors have the potential to send cautionary signals during a crisis and are, consequently, deployed in numerous places.

* Research Scholar, Faculty of Computer Science and Engineering, Department of Computer Science and Engineering, Sathyabama University, Chennai E-Mail:ntharminie@gmail.com,

** Professor, Department of Computer Science and Engineering, 2Vellammal Engineering College, Chennai, Tamil Nadu, India pandiandurai@gmail.com

The huge array of sensor nodes comprising a WSN is power-driven by batteries and supplied with intelligent, data dispensation and radio communication components withlimited range. Immensely popular WSN applications range from monitoring the environment and home automation to rather more challenging ones in defense areas including battleground surveillance, target and tracking the target systems.

WSNs are vulnerable to assorted network-level attacks, chiefly due to the lack of any kind of physical protection. The memory chips of the sensor nodes suffer from various memory read-outs susceptibilities, even if they are equipped with in-built tamper proof systems. Key management - an essential mechanism that ascertains network service security and WSN applications - can be described as a group of procedures and methods supporting main businesses and maintaining ongoing key rapport between legitimate parties in accordance with security policies. As sensor nodes in WSNs have restrictions imposed on them in terms of computing capability and memory power, security solutions proposed for other networks are not applicable to Wireless Sensor Networks. To create, distribute and maintain secret keys is the main aim of vital management in WSNs so as to provide solutions for the issues related to it. Therefore, mechanisms for reliably distributing and managing the keys are central to the security of WSNs.

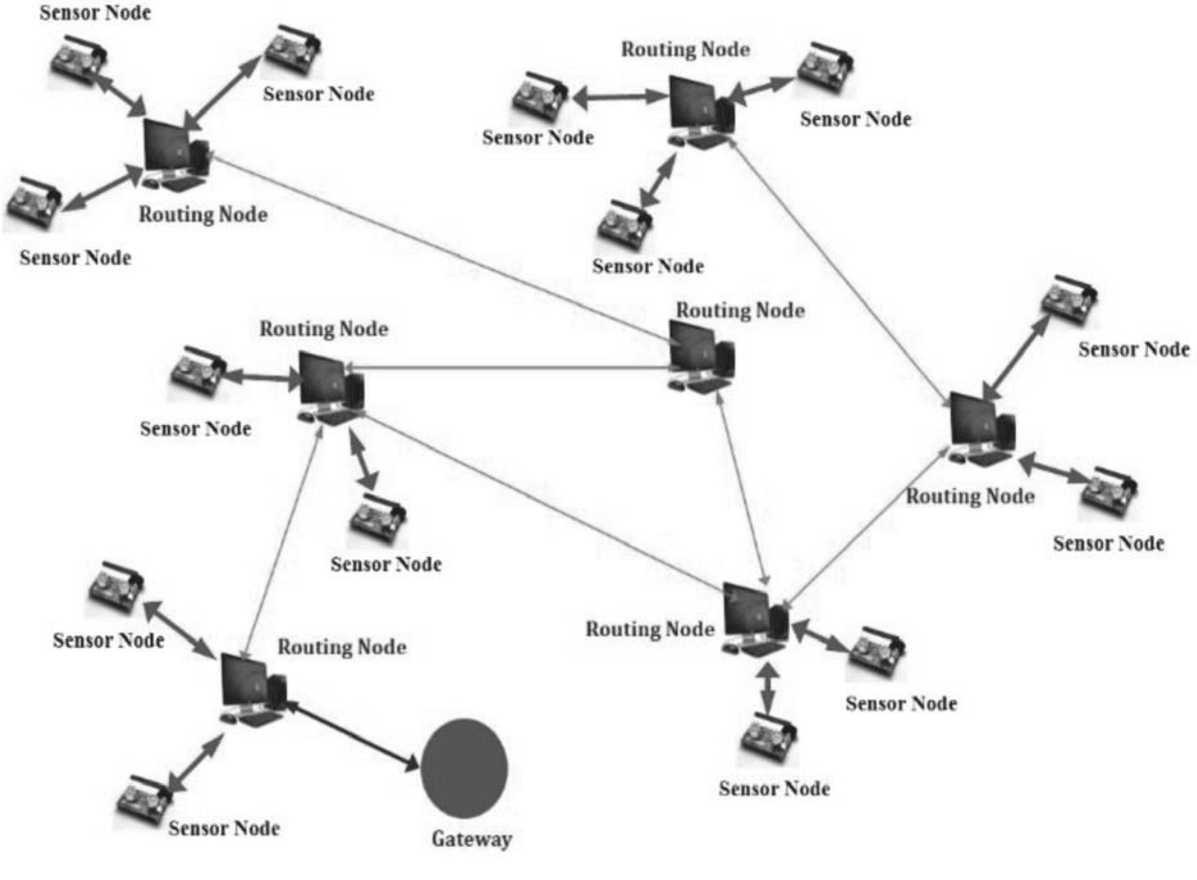

Fig. 1. Model Design of a Wireless Sensor Network

The increasing popularity of key management systems for WSNs has kindled strong interest in current scientific literature, thanks to which several key management techniques are being proposed for WSNs. These can be categorized into two classes, static and dynamic, owing to their potential to revise sensor nodes' cryptographic keys in the course of their runtime (re-keying). The former works on the theory of key pre-distribution, and the keys are refreshed for the entire network's life span. Nevertheless, the probability of attacks on cryptographic keys increases considerably, given that they are used for long periods of time. Cryptographic keys are revitalized all through the network's lifetime in the latter, the dynamic key management scheme, and considered adept in sensor networks. A set of procedures is utilized to execute re-keying, sporadically or on requirement, depending on the network's requirements. This method considerably augments network survivability and resilience because the compromised nodes' keys are withdrawn in the course of re-keying.

Key management schemes that are dynamic must assign cryptographic keys protectively, wrecking the activity of malicious nodes inside a network. The existing secret key of a sensor node which is compromised should be cancelled if the node in question is detected, and a latest one generated and dispensed to related sensor nodes, apart from the one that is compromised. It is also enviable for a dynamic key management system to preserve secrecy forwards and backwards and resist collusion between the nodes that joined recently and the affected ones. Further, flexibility beside node capturing and node replica should be delivered.

Once the malicious sensor nodes are identified, an effectual solution must be arrived at so as to have them withdrawn quickly from the network to avert a situation where a compromised node diverts network behavior by means of bogus data insertion or data modification of nodes that are trusted.

This segment reconsiders modern key management schemes that are dynamic for WSNs. Generally, a centralized key controller is engaged in the generation or distribution of a new key, and almost all dynamic key management schemes are either distributed or centralized. Alternatively, centralized dynamic key management may be grouped based on network, hierarchical network or heterogeneous network and on the structures of their network.

Dynamic key management which is distributed is a group of procedures where there is no re-keying of sensor nodes, thanks to the lack of a central administration. Instead, key management is administered by numerous key controllers which is predetermined or assigned dynamically. Dynamically distributed key management systems evade failure and permit improved network scalability, though errors in design errors may occur, since affected sensor nodes can take part in the process of evicting the nodes. Depending on cryptographic primitives, dynamic key management systems that are distributed are divided on the basis of EBS, polynomial secret-sharing and deterministic sequence number.

The remaining part of the paper is structured thus: Section II focuses on a literature survey of wireless sensor networks and security management, Section III on the proposed method of this paper, Section IV on results and implementation and Section V on the conclusion and upcoming work.

2. RELATED WORK

ROL, a novel route optimization based on cluster and load-balancing protocol, is presented. This utilizes different quality of service (QoS) metrics to attain the requirements of the application. Numerous applications are combined in ROL, particularly to offer comprehensive solutions that extend network life span, ensure delivery on time and enhance robustness of the network. An algorithm titled nutrient-flow-based distributed clustering (NDC) is proposed for balancing the load, working effortlessly with every clustering algorithm in most cases. Simulation results prove that the ROL/NDC provides superior network lifetime, as against other schemes [1].

WSNs that host multiple applications are widely preferred to ones that cater to a solitary application. During the process of allotting sensor nodes to requests of the application, the significance of using information about the application’s distinctiveness and network status is comprehensively studied. Several static and dynamic allocation algorithms are explored. Simulation results show that the life span of a WSN can be successfully increased [2] by utilizing information regarding its applications and condition.

ITS (intelligent transportation systems) are sophisticated applications meant specifically for the transportation industry. A key development therein is the ETC (electronic toll collection), facilitating efficient and swift toll collection. It is, however, prone to attacks in the form of eavesdropping, interfering, and tampering. A chaotic stream cipher-based cryptographic scheme to secure protected data communications over a WSN is suggested. This method permits ITS to effectuate key negotiation and data encryption among sensor nodes in a WSN. Experimental results prove that data transmission between wireless sensor nodes could be protected from attacks [3].

We discuss the issue of secure communication between distant nodes when keys are transmitted by compromised nodes. Therefore, a key distribution scheme known as the key distribution using fragmentation and assimilation (KDFA) is proposed. Here, the actual key is divided into fragments by a sender node and sent via an intermediate actor node. KDFA is comprised of KDP (key distribution protocol) and KFA (key fragmentation algorithm). The implementation of KDFA is specified and officially verified using Rubin logic. Simulator NS-2.35 is used and the results prove that KDFA is flexible against compromises by the actor node and key exposure [4].

Key management plays a major role in protecting WSNs from assorted attacks. A basic key management protocol for WSNs, along with a protocol based on the Diffie-Hellman algorithm, is recommended. This method meets energy efficiency requirements and controls the detrimental impact on security brought on by a captured node. The protection of the master key, key revocation and authentication mechanism are also discussed. The performance of the method is examined from the point of computational efficiency, storage requirements, cost of communication, and its capability to protect WSNs from various attacks. Finally, the direction of the research is also provided [5].

WSNs are extensively used in civil, military and commercial fields because of their adaptability and the low costs incurred. When compared to traditional networks, however, WSNs are confronted with resource constraints in the form of hardware and are consequently more vulnerable to security threats. The progress of research on sensor network security issues is tabled from the point of view of key management, authentication, and secure routing, it is scrutinized and observations appended along with future work and the direction of this field [6].

A dynamic security assessment method is recommended, depending on threshold cryptography in MANET, to examine the safety of distributed trust third-party (TIP) applications. The attacking process is studied and an attack model built using a stochastic process approach. A dynamic evaluation model is also presented to provide the proper value of the threshold. In addition, the security influence of the threshold value on diverse distributed CA schemes is analyzed and given here, the analysis being in line with theoretical conclusions drawn in previous papers. The results are helpful in building MANET security and measuring and evaluating network security performance [7].

The most favorable key generation issues for a entry security scheme in MANET are investigated. The issue is modeled by a closed discrete-time queuing method with L queues connected arbitrarily to K servers (K nodes have to be make contact for key construction). The problem is treated as one to do with resource allocation. The class of MBCC (most balancing credit conserving) policies is introduced and their mathematical classification provided. By utilizing active coupling arguments, we prove that MBCC policies are the best of the entire key-generation policies [8].

Nodes in a network are responsible for maintaining data reliability and confidentiality. A lot of schemes using key management are executed so as to achieve the objective of secure communication in MANETs. A composite identity and trust-based model (CIDT), which is a personalized DSR routing protocol determined on a public key, material identity and node's trust is proposed for accomplishing secure data transfer through wireless channels,. In order to validate a node, a trust factor apart from its key pair and distinctiveness is utilized. The generation of a valid certificate of node authenticity is necessary for the node to complete communications in the network [9].

Nodes in a MANET have limited resources and, therefore, tend to misbehave so as to conserve resources, influencing the performance of the whole network as a result. Therefore, a method wherein a MANET is set in a structure of zones and clusters is recommended. The static agent acts as a central node and each zone has a zonal agent. The introduction of zonal agents makes this system an improvement over mobile agent-based architecture. Consequently, selfish and malicious nodes are detected by the system with fewer information exchanges within nodes [10].

A solution is mooted to detect and avoid black hole attacks and guarantee protection of transmitted packets simultaneously, efficiently using the resources of mobile hosts, the results demonstrate that aspects such as node strength and constancy - defined by mobility, pauses in time, and existing battery power - determine the evaluation of trust where all nodes are concerned. The degree to which a node can be trusted forms the basis for selecting the most reliable transmission route. In relation to throughput, safe routing, and effectively using the resources, simulation results prove that the solution enhances performance [11].

A proposal to develop a trust-based QOS protocol (TBQP) to enhance and protect MANETs by means of a meta-heuristic genetic algorithm is examined. The genetic algorithm helps maintain the quality of service (QOS) by choosing the shortest possible route, thereby maximizing performance. Of late, QOS issues have been resolved to a considerable degree through meta-heuristic algorithms such as GA (genetic algorithm), NN (neural networks) built on AI (artificial intelligence), PSO (particle swarm optimization) and SA (simulated annealing). Ad hoc networks usually face threats in the form of attacks by malicious nodes. These attacks can be handled by the trust application and the security of the networks assured [12].

Packet dropping attacks by malicious node(s) is considered a likely scenario in MANETs. An interference detection mechanism utilizing fuzzy-logic for detecting packet dropping attacks in MANETs, and eliminating malicious nodes to safeguard the resources is proposed. The QualNet simulator 6.1 and Mamdani fuzzy inference mechanism simulate this system. Results shows that this system is most competent at identifying dropping attacks resulting in a favorable positive rate and reduced false positive [13].

A key disadvantage in a MANET is the lack of a centralized monitoring system, rendering it vulnerable to assorted attacks by malicious nodes. A new multi-hop recommendation-based trust management method called TRUISM is considered, and the popular Dempster-Shafer theory adapted to combine recommendations efficiently from varied devices. A new recommendation-routing protocol called 'buffering on-the-fly' is established to decrease the volume of traffic engendered by the recommendations in question. Experimental results prove that in the presence of opposing recommendations, the model performs well and also guarantees speedy and scalable sharing of trust-based information by decreasing the packet flow on the whole [14].

The enhanced adaptive acknowledgment (EAACK), a phenomenon of an intrusion identification scheme, is discussed below, with ACK, S-ACK (secure ACK) and MRA (misbehavior report authentication) being its components. All packets are verified and signed digitally to thwart the passage of forged acknowledgement packets. The system utilizes a one-hop ACK that usually enhances misbehavior detection rates but cannot, however, specifically mark a misbehaving node. Sometimes, though, nodes that behave well may also be part of a misbehaving link. The Diffie-Hellman key exchange algorithm is considered by the system to eradicate the need for pre-distributed keys [15].

An IDS (intrusion detection system), used to detect malicious attackers, comprises end-to-end feedback, monitoring in watchdog mode, activity-based eavesdropping and a status-based solution. The suggested approach recommends the implementation of hybrid cryptographic techniques to decrease network overhead. The instant key generation mechanism (IKGM) is a new, crucial exchange system launched to eliminate the necessity for key pre- distribution. The key is encrypted at every node to augment performance against modern procedures, in addition to offering a better malicious behavior detection rate [16].

The focal point of discussion is security threats confronting AODV, the most familiar MANET routing protocol of all, as a consequence of black hole and flooding attacks. A study is conducted in NS-3 simulator to evaluate the performances of preventive methods such as FAP and AMTT, in the event of MANETs finding themselves susceptible to flooding or black hole attacks. Performance is evaluated based on throughput, delay in messages and routing overhead with an increase in flooding attacks, average packet delay and increase in routing overhead. In comparison, black holes have a lesser packet drop ratio. [17].

Attacks in terms of denial of service are potential threats for wireless networks, guzzling the resources of the system and separating genuine network users as well. A gray hole attack is one of such a kind and happens when a compromised node drops acknowledged data packets throughout the route- discovering process. Based on two Bayesian classification models, Bernoulli and multinomial, to detect attacks of this sort, a new approach is proposed. Simulation results show that the deliberate dropping of packets can be completely detected with false starts of lower level [18].

Security is a prime concern in a hostile environment, and a MANET poses a huge challenge to security design due to its unique characteristics. The use of a symmetric key HAMC (message authentication code) for secure data transmission - where only authorized personnel are permitted and communication data secured in the network as a consequence- is discussed. The hash message authentication code is used for secure data transmission, wherein the message is readable only after it is decrypted. Decryption is done at the destination since only the code is aware of the secret decrypting key [19].

A privacy protecting secure and energy-efficient routing protocol (PPSEER) is suggested to offer a protected and energy-saving routing protocol. The classification of network nodes, based on their energy levels, takes place in this protocol, while encryption is carried out based on the group's signature. It also contains a supplementary secure parameter like a secret key, recognized only by the sender and recipient node, and maximum transmission power. The protocol not only intensifies message privacy, but also maintains the node's energy efficiency [20].

Providing security is a taxing issue in today's internet- connected life, especially with the rising use of sensor nodes. Offering effective key management schemes with their ability to extend a network's lifetime is necessary, as a result of limitations imposed on sensor nodes. An analysis of current key management schemes recommended for dynamic WSNs is examined. No scheme, however, is perfect enough to satisfy all evaluation metrics. They have specific characteristics of their own, making them ideally suited to specific applications [21].

A network defense management which is also adaptive is analyzed for defying intelligent attacks and selective capturing, with its plans to severely damage the fundamental data release function of a base station-based WSN. With selective capturing, rivals tactically confine sensors and convert them into attackers within. In the case of smart attacks, an attacker from inside is capable of carrying out dangerous incursions to avoid detection. A model-based analysis tactic is developed with justification to discover the best defense protocol background under which sensor network life span is increased against selective capturing and intelligent attacks [22].

Five essential data flow techniques - service operation and communication, network initialization, implementation, placement and administration which requires added prop up from middleware node is discussed to guarantee safe and protected multi-user nodal communications. In order to preserve data flow, this paper presents the rudiments, design, execution and incorporation of the necessary middleware mechanisms and, further, expounds on their communication and reliance. The assessment shows that sensor nodes with limited resources are capable of supporting protected sharing of nodes [23].

3. PROPOSED WORK

The suggested mathematical representation for energy utilization, established on CL-EKM with several specifications, is associated with nodal movements. This representation will be used to approximate the correct value for the Thold and Tback, and is established on velocity and the trade-off between energy utilization and security levels.

The recommended model is tough against factors such as node compromise, duplication and imitation attacks, also protecting data privacy. The results reveal the efficiency of CL-EKM in WSNs which contain limited resources.

Fig 2 shows the proposed model architecture with the solid line indicating rare (or only one) transactions. For example: ack is only one for all packets. The dotted line indicates frequent transactions.

Pk	–	Public Key
D	–	Destination
dn	–	Datagram (small size of data)
A	–	Acknowledgement
T	–	Tail node

A. Formulating a mathematical representation for energy utilization based on CL-EKM with different parameters linked to nodal movements - Selecting suitable sensors for transferring data:

This segment focuses on how to calculate key factors, connected with spatial connection between sensors, affecting the selection of sensors. Another major issue is the sensor nodes' left over energy. A sensor node is considered suitable based on the parameters considered; but, that sensor may be deficient in the energy needed for transferring the data. As a result, considering the balance energy of sensors ei and the value attained, the selection mass for selecting a suitable sensor for transferring data is achieved by

$$M_i = U_i + e_i$$

If the value of Mi is higher in a sensor node, it is considered more suitable for transferring data to the target node. Here, our main aim is to compute the least number of sensor nodes required for transferring data, followed by relevant instructions. Adhering to the instructions given, sensors not appropriate for transferring data are eliminated. This results in energy being saved as it eliminates the need to send inessential data.

Described below is the error function :

$$\varepsilon_i = d_i - y_i$$

di indicates the least energy needed for sending data.

The LMS filter is used to choose appropriate sensors for ransferring data that will decrease the value of $\varepsilon_1{}^2$. If there is an incident in the network, sensors inside the radius of the event collect it and the M value in the sensors is evaluated.

We consider $[M_1,...M_m]$ for each sensor and is assigned [W0, W1,W2]. Thus the output is as below:

$$yi = k = 1\text{n Mk Wk} + \text{W0}$$

$$W_{k+1} = W_k + \mu\, \varepsilon_i M_k$$

Then, by reducing the target function $\varepsilon_1{}^2$ the selected nodes for transferring data are chosen. The pseudo-code for choosing the finest set of nodes are:

```
For each                                   $n_i \in V(S)$
                            Initial weight $w = [W0, W1,W2]$
Calculated                                 $yi = k = 1nMkWk + W0$
If $y_i > 0$ select $n_i$, calculated      $\varepsilon_i = d_i - y_i$
Adapt weight                               $W_{k+1} = W_k + \mu\, \varepsilon_i M_k$
Else reject $n_i$

Repeated to $\varepsilon_1^2 \leftarrow \varepsilon_1^2$ min
```

B. Proposed algorithm

A -> public key entity

PA -> public key for entity A

G_1 – multiplicative group with specific prime number order (like *q*)

H – Hash function

N – Length of plain text.

Encryption : To encrypt $M \in M$ for entity with identifier $ID_A \in \{0, 1\}^*$ and public key $P_A = \{X_A, Y_A\}$, perform the following steps:

1. Verify that $X_A, Y_A \in G^*_1$ and that the equality $e(X_A, P0) = e(Y_A, P)$ holds. If not, output and abort encryption.
2. Calculate $Q_A = H1(ID) \in G_1{}^*$.
3. Choose a random $\sigma \in \{0, 1\}^n$.

4. Set $r = H_3(\sigma, M)$
5. Calculate and output: $C= \{rP, \sigma \text{ XOR } H_2(e(Q_A,Y_A)r), M(H_4(\sigma)\}$.

Decryption : If the cipher text $C=\{U,V,W\} \in C$. To decrypt the cipher text using the private key S_A:

1. Compute $V \text{ XOR } H_2(e(S_A,U) = \sigma'$.
2. Compute $W \text{ XOR } H_4(\sigma') = M'$
3. Set $r' = H_3(\sigma', M')$ and test if $U = r'P$. If not, output and reject C.
4. Output M' as the decryption of C.

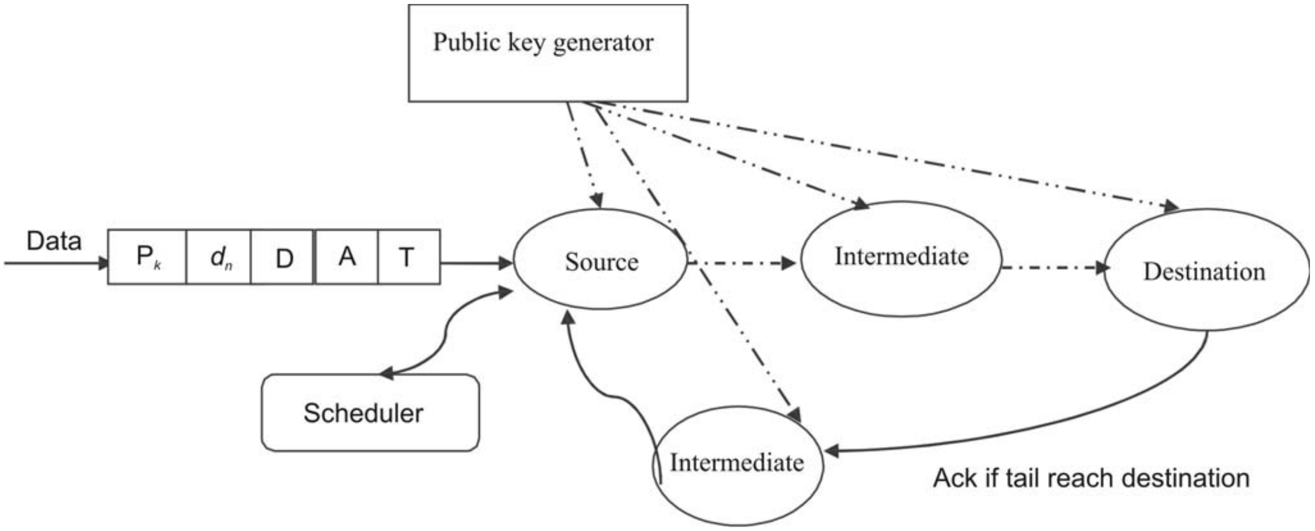

Fig. 2. Proposed Model Architecture

By utilizing PA and IDA, supposing C a valid encryption of M, then interpreting C will result in the output M' = M. We note that W can be replaced by $W = E_H (\sigma)$ (M), where E represents a semantically protected symmetric key encryption scheme.

4. RESULTS AND IMPLEMENTATION

We consider 35 nodes to experiment with, of which 20 are active and ready to send data transfers. Initially, all nodes get the public key. The nodes ready for data transfer encapsulate the following data such as public key, datagram, and destination. During data transaction, nodes send the encapsulated packet. Each node de-capsulates and verifies the destination and keys. Prior to being sent, data are split into data packets (data = *n* data packet + tail packet). The tail packet plays a key role. If the packet is a tail packet, all the datagram is combined into a single piece of data at the destination. The acknowledgement is then sent to the source. If the datagram is not converted into data, we assume that the data packet is lost, with an attacker tracking the data transfer. This algorithm cuts through data traffic and data delay.

The Fig.3 illustrates the deviation of data transfer delay by nodes with regard to various data transactions. In the x- axis, the time required for transfer and in the y-axis, the number of packets transmitted is plotted. There are four different-coloured lines indicating that miscellaneous transactions commenced at the same time. The red line shows the maximum data transfer delay since it began last. The green started first, when there was no traffic. The blue began after the green, by which time some traffic had been generated by the green. When the yellow starts, it will find itself up against traffic from the green and the blue.

The Fig.4 illustrates the deviation of data packet loss by nodes in respect of assorted data transactions. In the *x*-axis, the total packets sent and in the *y*-axis, the total packets received are plotted. There are four different-coloured lines, indicating that diverse transactions started at the same time. The red line shows the maximum data loss, as it started last. The green started first, when there was no traffic. The blue started after the green when some traffic had been generated by the green. The yellow will start next, facing traffic from the green and the blue. An increase in traffic is accompanied by a corresponding increase in data loss.

The Fig.5 illustrates the deviation of throughput with various data transactions by nodes. In the x-axis, the total packets sent and in the y-axis, the total packets received are plotted. There are four different-colored lines, indicating that diverse transactions started at the same time. The yellow line, having started last, shows maximum throughput. The green started first at a time when traffic was zero. The blue started next to the green, by which time some traffic had been generated by the green. Next, the yellow will start, facing traffic from the green and the blue. If traffic increases, data loss also increases and, as a consequence, throughput decreases.

5. CONCLUSION

Physical factors such as light, temperature, humidity and vibrations are managed by a WSN made up of a huge array of sensor nodes extended over different geographical areas. A mathematical representation for energy utilization on a CL- EKM basis, in terms of nodal movements, is proposed. This representation is used for estimating the correct value of the Thold and Tbackof parameters on the basis of velocity and the desired trade-off between energy utilization and protection levels. The suggested technique is safe against compromising of nodes, duplication and imitation attacks, and also ensuring data privacy. The results show the eûciency of CL-EKM in WSNs which has limited resources. The NS2 simulator is used to implement this efficient method. 35 nodes are considered for experimentation, of which 20 are active.

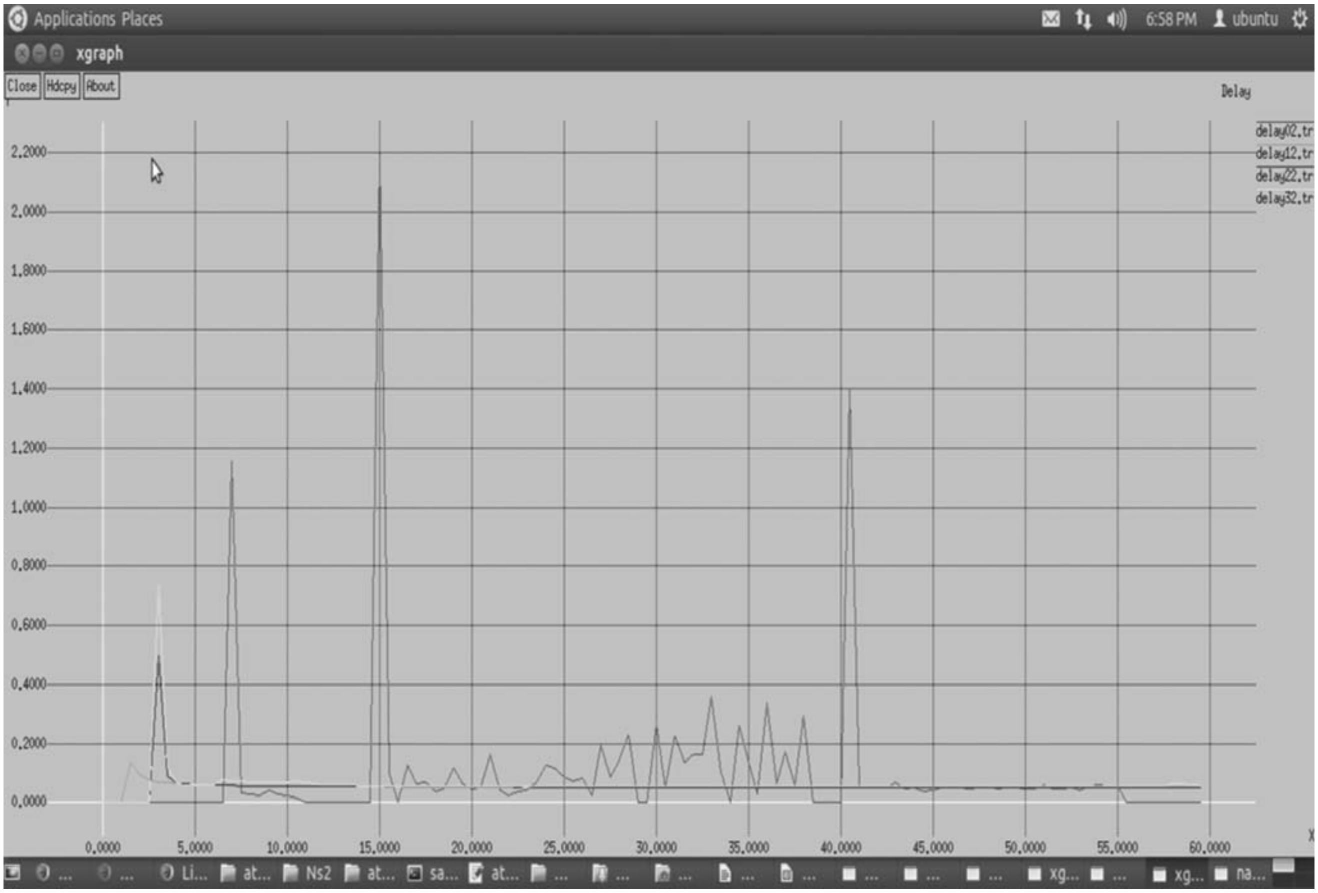

Fig. 3. Deviation of data transfer delay.

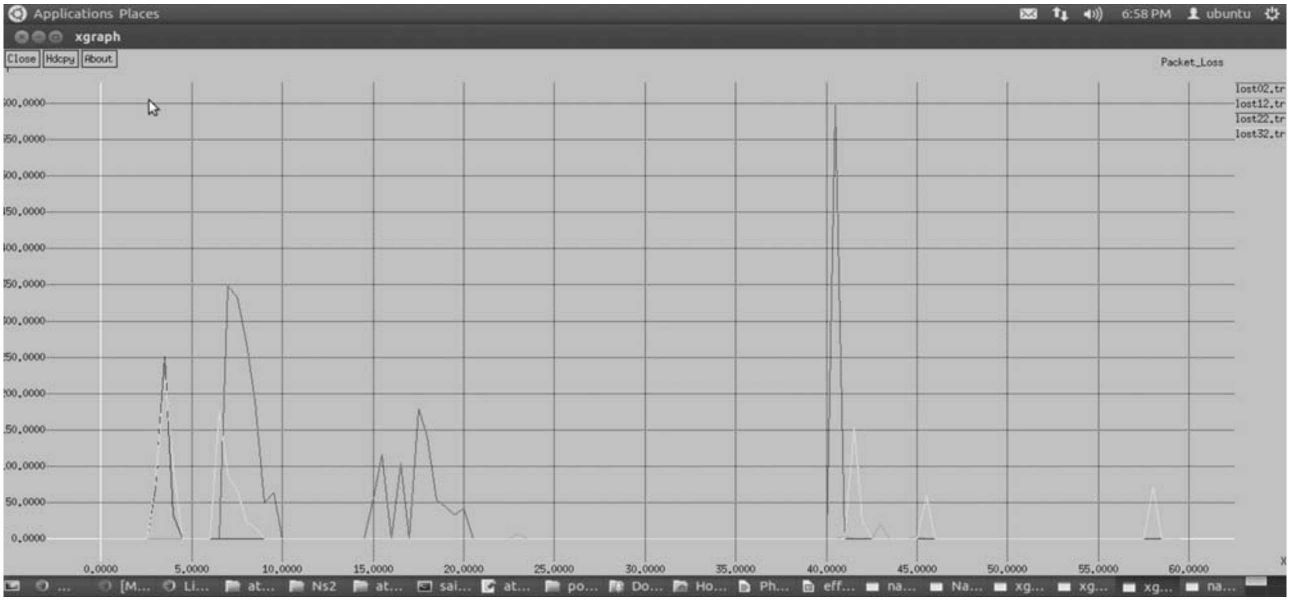

Fig. 4. Deviation of Data Packet Loss.

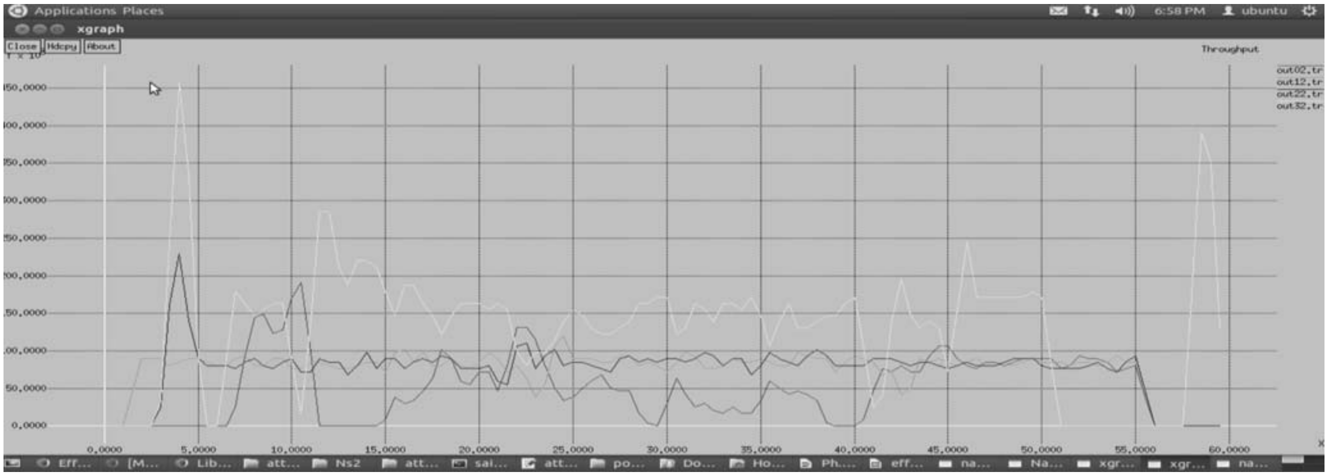

Fig. 5. Deviation of throughput.

The nodes ready for data transfer encapsulate data comprising the public key, datagram, and destination. Nodes send the encapsulated packet during data transactions, with each node de-capsulating and verifying the destination and keys. The data are split into a data packet (data = *n* data packet + tail packet) before they are sent. All datagram is combined into a single unit of data, ending at the destination if it is a tail packet, and the acknowledgement sent to the source. If the datagram does not convert into data, then we assume that the data packet is lost and an attack of some sort is imminent during data transfer. This algorithm overcomes data traffic and data delay. Our future work focuses on the possibility of the SET-IBS and SET-IBOOS protocols as they relate to obligations in terms of security and withstand scrutiny against different attacks.

5. REFERENCES

1. Hammoudeh, Mohammad, and Robert Newman. “Adaptive routing in wireless sensor networks: QoS optimisation for enhanced application performance.” *Information Fusion* 22 (2015): 3-15.
2. Kaur Kapoor, Navdeep, Shikharesh Majumdar, and Biswajit Nandy. “Techniques for Allocation of Sensors in Shared Wireless Sensor Networks.” *Journal of Networks* 10, no. 01 (2015): 15-28.
3. Zhang, Wei, Shanyu Tang, Liping Zhang, Zhao Ma, and Jun Song. “Chaotic Stream Cipher-Based Secure Data Communications over Intelligent Transportation Network.” *International Journal of Antennas and Propagation* 2015 (2015).

4. Ghafoor, AtaUllah, Muhammad Sher, Muhammad Imran, and Abdelouahid Derhab. "Secure Key Distribution Using Fragmentation and Assimilation in Wireless Sensor and Actor Networks." *International Journal of Distributed Sensor Networks* 501 (2015): 542856.

5. Cui, Baojiang, Ziyue Wang, Bing Zhao, Xiaobing Liang, and YueminDing. "Enhanced Key Management Protocols for Wireless SensorNetworks." *Mobile Information Systems* 2015 (2015).

6. Yang, Qiuwei, Xiaogang Zhu, Hongjuan Fu, and Xiqiang Che. "Survey of Security Technologies on Wireless Sensor Networks." *Journal of Sensors* (2015).

7. Haibing, Mu, and Zhang Changlun. "Security evaluation model for threshold cryptography applications in MANET." In *Computer* Engineering and Technology (ICCET), 2010 2nd International *Conference on*, vol. 4, pp. V4-209. IEEE, 2010.

8. Al-Zubaidy, Hussein, Ioannis Lambadaris, Yannis Viniotis, Changcheng Huang, and Ren-Hung Hwang. "Optimal Key Generation Policies for MANET Security." In *Global Telecommunications Conference (GLOBECOM 2010), 2010 IEEE*, pp. 1-6. IEEE, 2010.

9. Khatri, Pallavi. "Using identity and trust with key management for achieving security in Ad hoc Networks." In *Advance Computing Conference (IACC), 2014 IEEE International*, pp. 271-275. IEEE, 2014.

10. Talreja, Rahul, and Vimla Jethani. "A vote based system to detect misbehaving nodes in MANETs." In *Advance Computing Conference (IACC), 2014 IEEE International*, pp. 391-394. IEEE, 2014.

11. Biswas, Santosh, Tanumoy Nag, and Sarmistha Neogy. "Trust based energy efficient detection and avoidance of black hole attack to ensure secure routing in MANET." In *Applications and Innovations in Mobile Computing (AIMoC), 2014*, pp. 157-164. IEEE, 2014.

12. Zafar, Sameena, and M. K. Soni. "Trust based QOS protocol (TBQP) using meta-heuristic genetic algorithm for optimizing and securing MANET." In *Optimization, Reliabilty, and Information Technology (ICROIT), 2014 International Conference on*, pp. 173-177. IEEE, 2014.

13. Chaudhary, Arun, Ajit Kumar, and Vijay N. Tiwari. "A reliable solution against Packet dropping attack due to malicious nodes using fuzzy Logic in MANETs." In *Optimization, Reliabilty, and Information Technology (ICROIT), 2014 International Conference on*, pp. 178-181. IEEE, 2014.

14. Bijon, Khalid Zaman, Md Mohaiminul Haque, and Ragib Hasan. "A trust based Information sharing model (TRUISM) in MANET in the presence of uncertainty." In *Privacy, Security and Trust (PST), 2014 Twelfth Annual International Conference on*, pp. 347-354. IEEE, 2014. [15]. Sandhiya, D., K. Sangeetha, and R.S. Latha. "Adaptive ACKnowledgement technique with key exchange mechanism for MANET." In *Electronics and Communication Systems (ICECS), 2014 International Conference on*, pp. 1-5. IEEE, 2014.

16. Dhanalakshmi, K. S., B. Kannapiran, and A. Divya. "Enhancing manet security using hybrid techniques in key generation mechanism." In *Electronics and Communication Systems (ICECS), 2014 International Conference on*, pp. 1-5. IEEE, 2014.

17. Hassan, Asif, and Milena Radenkovic. "Simulation of security attacks and preventions on AODV protocol in ns-3." In *Innovative Computing Technology (INTECH), 2014 Fourth International Conference on*, pp. 158-163. IEEE, 2014.

18. Rmayti, M., Youcef Begriche, Rida Khatoun, Lyes Khoukhi, and Dominique Gaiti. "Denial of Service (DoS) attacks detection in MANETs through statistical models." In *Global Information Infrastructure and Networking Symposium (GIIS), 2014*, pp. 1-3. IEEE, 2014.

19. Senthil Kumar, A., and E. Logashanmugam. "To enhance security scheme for MANET using HMAC." In *Current Trends in Engineering and Technology (ICCTET), 2014 2nd International Conference on*, pp. 467-471. IEEE, 2014.

20. Devi, E. Ahila, and K. Chitra. "Security based energy efficient routing protocol for Adhoc network." In *Control, Instrumentation, Communication and Computational Technologies (ICCICCT), 2014 International Conference on*, pp. 1522-1526. IEEE, 2014.

21. Erfani, Seyed Hossein, Hamid HS Javadi, and Amir Masoud Rahmani. "Analysis of Key Management Schemes in Dynamic Wireless Sensor Networks." (2015).

22. Al-Hamadi, Hamid, and Ing-Ray Chen. "Adaptive Network Defense Management for Countering Smart Attack and Selective Capture in Wireless Sensor Networks." (2015).

23. Maerien, Jef, Sam Michiels, Danny Hughes, Christophe Huygens, and Wouter Joosen. "SecLooCI: A comprehensive security middleware architecture for shared wireless sensor networks." *Ad Hoc Networks* 25 (2015): 141-169.