Efficient key Management System using Channel Response in Wireless Sensor Network

Manikandan G, Sakthi U

Abstract: There are challenges abound for key management in wireless sensor networks. The importance of key management gets highlighted when the network gets scaled up without the availability of enough resources and new kind of threats in the form of node capture emerge. The economic viability of such schemes are usually high as the increase in security is directly proportional to the computational complexity, thus attributing to the high cost. In the wireless sensor infrastructure, nodes get connected with each other in wireless medium and can enter and exit the network at their will. Such aspect of entering and exiting paves the way for malicious nodes too to enter in to the network, making the entire network vulnerable to several types of attacks. One of the prominent attack is network jamming where the transmission lines gets jammed blocking the free flow of data as well as corrupting it. Such attacks on node and data transmissions can be avoided by increasing the security afforded to the entire WSN. In this regard, a novel key generation algorithm has been proposed in this paper using channel response technique, where the data hops from one channel to another in its transit from the source node to the destination node securing it from attacks. The Leap and Stop algorithm has been applied for channel hopping thus ensuring that the data traverses only for a small duration in each channel before hopping to the other channel. The channel hopping technique minimizes the probability of attack since before an active channel could be successfully predicted by the attacker, it becomes inactive and another channel gets activated. This channel hopping process continues till data reaches the destination safely without getting corrupted. The proposed approach had been compared for its efficiency and performance with Secure Key Generation using Frequency Selective Channels (SKGFSC) protocol and the results had been shown therewith.

Keywords: wireless sensor network, channel response, jamming, Security, key management, SKGFSC protocol.

I. INTRODUCTION

Wireless sensor networks comprise of numerous sensors that are configured to sense, monitor and collect data related to various events and transmit the collected information to a specified destination. They are handy enough to collect real time data and aggregate it and forward the same for further processing. Sensors are in huge demand for surveillance type of applications. Wireless sensor networks are applied in varied domains ranging from military to domestic, forest to farming [1]. The primary contention issue in such networks is the open transmission of data which could easily come under various types of attacks.

Enforcing security in wireless domains depend on the size of the sensors, battery power and memory required for the sensors to carry out the task assigned to them. [2]. In wireless sensor networks, cryptography, key management, secure routing, data collection and aggregation, intrusion detection and ensuring trust among the sensor nodes are considered as the primary issues related to security that must be effectively taken care of. Attacks both in the form of passive as well as active can be launched not only on the sensor nodes that are transmitting data but also on the data that is transmitted as well [2]. Adversaries could pop out from both external as well as internal fronts. The internal node could be under the control of the attacker. Protection could be afforded from such adversaries through the security keys. By deploying secure key management techniques at the sensor nodes, cluster heads and base stations, the exchanged data could be made more secure in the wireless sensor networks [20].

II. MOTIVATION

Key management is a challenging task to be realized in the wireless sensor networks. Security risks increases manifold when the sensor networks are deployed in hostile environments. Setting a secure communication and distributing the security keys is a major task of contention for researchers in the wireless sensor domain. Increasing the resilience of the network by thwarting the active jamming attack without consuming more memory is the main motivation behind this work. A skillful adversary can very well compromise the secret key as well as the encryption randomness employed in the network by intercepting the network communication. Therefore by incorporating the key management approach in the wireless sensor networks, data confidentiality, integrity, freshness, availability, and authentication of node as well as the data exchanged can be efficiently upheld.

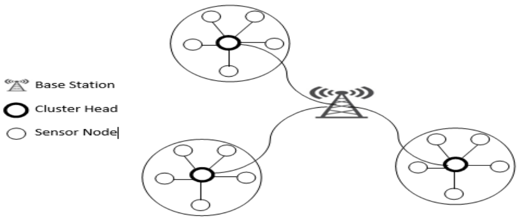
Manuscript received on March 15, 2020.
Revised Manuscript received on March 24, 2020.
Manuscript published on March 30, 2020.

* Correspondence Author

Manikandan G*, Research Scholar, Department of Computer Science and Engineering, Sathyabama Institute of Science and Technology, Chennai,TamilNadu,600119,India Email: maniprofessional@gmail.com

Sakthi U, Professor, Department of Computer Science and Engineering,St.Joseph's Institute of Technology, Chennai, TamilNadu India. Email: sakthi.ulaganathan@gmail.com

Retrieval Number: F9530038620/2020©BEIESP
DOI: 10.35940/ijrte.F9530.038620
Journal Website: www.ijrte.org



.

Fig .1.WSN Architecture

Sensors: The performance of a sensor is constrained by the restrictions imposed by power, computational capability, memory, data manipulating prowess and its ability to engage in successful short distance transmission. As mentioned in fig.1 the sensors are configured to exchange information with the cluster head and not with any other sensors. Once deployed, they remain static.

Cluster Head: Nodes that have inherently high energy, high performance processors and huge memory are usually designated as cluster heads. A cluster head collects information from a set of sensor nodes and transmits it to a base station.

Base Station: General assumptions pertaining to a base station is that they are secure enough and trusted by all the nodes in the network. They are possessed with high computing and transmission power along with strong network coverage capabilities.

III. KEY MANAGEMENT SCHEMES IN WIRELESS SENSOR NETWORK

A key management scheme is deemed to be successful when it has the ability to thwart any attack on a highly vulnerable as sell as resource constrained sensor network. In wireless sensor networks [21], the key management schemes can be broadly categorized into static and dynamic types. The categorization is based upon the enabling of update feature of the administrative keys after they get successfully deployed in the network .

A.Static Key management schemes

This scheme is based on the assumption that, post the deployment of administrative keys in the nodes, they remain unaltered [17]. The administrative keys are created before deploying them and are assigned to nodes in a random manner or by following some deployment criteria and finally distributed to nodes. To begin communication with neighboring nodes, the administrative keys are overlapped for ascertaining whether they are capable enough to generate a direct pair-wise key. Links are handed over with the communication keys rather than the nodes. The previously established direct communication keys are used for establishing and distributing a newly generated communication key between two non-neighboring nodes and a group of nodes by propagating it on one link at a time between them.

B.Dynamic Key management schemes

The administrative keys keep constantly changing in dynamic key management schemes either based on demand or whenever code capture is detected [17]. The network's survivability feature gets enhanced through the dynamic scheme as any key that is captured is replaced immediately through a process called as rekeying. Scaling up of network can be effectively carried out using the dynamic scheme. Once new nodes are added up, the probability of network capture can be restricted. The rekeying mechanism applied in the dynamic key management scheme needs to be highly secure and efficient enough to withstand any probable attack.

IV. RELATED WORK

The following section throws light upon a range of key management protocols and their application in the wireless sensor networks.

Zhang et al [3] had proposed a secure and efficient hierarchical key management scheme (SHEKM) by taking into consideration of various security features that would be required in a wireless sensor network environment that needs to be satisfied. The authors, in their proposed approach had set up three different keys for encrypting the messages transmitted between the sensor nodes. A network key was created for encrypting the broadcast type of messages as well as for authenticating fresh nodes in network. A group key was created and shared among all nodes within a cluster and a pair wise key was defined and shared with specific pair of nodes that engaged in communication. The cluster heads in hierarchical WSNs were critical as they defined the network structure. A back up node for each cluster head had been designated to overcome any node compromise attack. The proposed approach was more economical with respect to the resources that were consumed and offered improved security to the network. A comparative analysis of the proposed approach with other existing key management approaches was conducted and the proposed approach was found to be highly efficient in the areas of key computation, exchange and storage Bhaskar et al [4] had studied the hierarchical wireless sensor networks and had observed that the wireless sensors deployed in such environments possessed several capabilities for achieving energy conservation. A wireless sensor network's security can be enhanced by designing efficient key management protocols that account for activities like key distribution, key withdrawal, generation of shared key and finally updating the generated keys. A notable constraint blocking the efficiency of the key management technique is the resource availability criterion. In order to maximize the resource utilization capability, the authors had proposed a key management technique based on Chinese remainder theorem. The key generation based on the proposed approach involved less computation and was found to be highly economical. The authors had also found practical results favoring storage, scalability features and efficiency to withstand various attacks. Security offered through the application of conventional cryptographic techniques in wireless sensor networks were highly impractical due to the fact that they consumed high energy, complex computations and involve high overhead. Suganthi et al [5] had proposed an efficient key management approach that offered high security to data in the wireless sensor environment. An efficient algorithm had been proposed for generating three keys for varied purposes for every sensor node to secure the transmitted information.

Retrieval Number: F9530038620/2020©BEIESP
DOI: 10.35940/ijrte.F9530.038620
Journal Website: www.ijrte.org

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

A shared key was generated for sharing the information between each node and the base station, a pair key for each sensor node that it uses while communicating with its neighbor and a group key that was shared by every node in the network. The proposed algorithm accounted for the efficient generation and updation of these three keys with involving the base station. An efficient polynomial function was designed for key computation during the key initialization stages.

New keys were immediately generated owing to changes in membership or on detecting node compromise attack activity in the network. The generated keys were also automatically updated periodically. The proposed approach was found to be highly energy efficient in successfully managing the issue of energy drain and created sufficient memory for operations related to storage. The attained security level was ascertained by testing the proposed technique against various security attacks and hence was found to be more suitable at un-manned areas. The proposed key management technique was highly efficient and accounted for comparatively less overhead than other existing techniques. An efficient key management approach had been proposed by Gupta et al [6] based on Blom's key agreement protocol that successfully overcame the aforementioned shortcomings. Practical observations conducted revealed that the proposed approach consumed less memory, accounted for less computational overhead and offered enhanced security to the network when compared with other approaches The application of wireless sensor networks in various domains had been constrained for want of additional security. Establishment of security keys between each pair of communicating nodes is highly challenging. Qin et al[7] had proposed an efficient identity based key management (IBKM) approach that successfully overcame the shortcomings identified. The authors had incorporated the Bloom's filter in their proposed approach for distributing the session keys as well as authenticating the communicating nodes with each other, offering excellent storage efficiency between the communicating nodes. Authentication in the proposed IBKM approach is done without involving the certificate authority. The practical observations carried out had revealed that the proposed IBKM approach involved less computational as well as communication overhead albeit maintaining the required security level when compared to other existing approaches. The communications taking place in the wireless network environment needs to be secured due the presence of high vulnerability in such networks. The sensors function independently which is in accordance to their configuration. The security keys to be applied for communication by the sensor nodes are stored in their respective memory which is highly vulnerable. This coupled with the resource restrictions makes the task of applying a simple encryption technique for protective purposes makes the task highly challenging. Kazienko et al [8] had proposed novel technique called SENSOR Lock for overcoming the above stated issues. The authors had demonstrated the feasibility of their proposed technique in carrying out secure symmetric key distribution that had successfully overcome the shortcomings of the stored key exposure issues. The node security was highly enhanced by the proposed approach that offered high resistance to node tampering type of attacks. Experimental results obtained through simulations showed that the proposed SENSOR Lock approach involves less processing overhead and consumed less power. In the numerous domains wherever wireless sensor networks are applied, key management turns out to be vital to establish trust among nodes and protecting the transmitted content. Du et al [9] had proposed an innovative key management technique that was based on Modular Arithmetic where the congruence property of the modular arithmetic was applied. Every sensor nodes stores a key seed in its memory using which it generates a unique key that it shares with its cluster head. Also a group key that is computed using the same key seed is shared with neighboring nodes in the network. The proposed technique brings down the storage requirement at each node. Updation of the key seed at each node is done swiftly. Comparing the proposed approach with other key management techniques, it was found that the proposed approach consumed less storage space and was strong enough to thwart node capture attacks. The mission critical applications where wireless sensor networks are applied, apart from demanding efficient energy management techniques, also stress the importance of security needs for the information exchanged. Zhang et al[10] had proposed a deterministic energy efficient key management technique that could be effectively applied in the resource constrained wireless sensor networks. In the proposed approach, apart from the generation and maintenance of pairwise key that could be applied between each sensor nodes, local cluster keys are also generated and maintained by each node for exchanging information with their respective cluster heads. A neighbor table is maintained by each sensor node where the keys are generated, stored, managed, transferred and updated accordingly. Utmost security had been afforded to the neighbor table at each sensor node. Any node can independently join, exit as well as rejoin the network and this had been done using elliptic curve digital signature algorithm. The proposed key management approach is of infrastructure-less type as it does not fall under either centralized or location based types. Since the proposed approach involves minimal computations, minimal exchanges and minimal storage, the overhead generated is comparatively less when compared with other existing key management techniques. Liang et al[11] had proposed a dynamic energy efficient key management technique for wireless sensor networks. Sensor nodes are clustered and are segregated in to specific number of virtual grids. Energy conservation is handled by enabling a single grid at any moment. The proposed approach applies a variety of techniques to achieve effective key management. The pair wise keys are generated by applying a common polynomial in tandem with a random number that could be used for effective communication between cluster heads. Similarly, a head polynomial in tandem with a random number is used for generating a pre-distribution key that could be applied for carrying out communication between active nodes with their respective cluster heads. The wireless sensor networks are best suited for hostile environments for data collection. A high level of security needs to be maintained at such environments. The transmitted information can be secured by generating security keys using cryptographic techniques. Construction of public key cryptosystem like RSA is not suitable in a wireless sensor domain due to the resource restrictions in each sensor node.

This could be complemented by applying symmetric cryptosystems where shared secret keys are applied. Messai et al [12] had proposed a novel key management technique that was adaptable to the demanding requirements of wireless sensor networks. The comparative analysis carried out between the proposed approach and other existing techniques showed that the proposed approach consumed less storage, was highly scalable and robust enough to overcome node capture type of attacks. Bechkit et al. [13] had stated that the wireless sensor network environment is highly sensitive and constrained with resource restrictions. A successful key management approach in such environment enhances the security of nodes by thwarting existing vulnerabilities. Design of any key management scheme should centre its design consideration on the future scalability aspect of the network where in such case it could be successfully applied to support the large network without any design modifications. An innovative key management technique had been proposed by the authors to support scalable networks with primary concern on security and connectivity issues. A novel unital design theory had been proposed where the unitals were mapped with the key pre-distribution parameters. Such mapping ably supported the network's scalability criterion and accounted for efficient key sharing. The authors had compared their proposed approach with other existing approaches based on parameters like scalability, storage overhead, network resilience, average secured path length and network connectivity. The results obtained were highly were found to be highly encouraging. Eltoweissy et al. [14] had demonstrated a key management model that had the capability to establish and maintain a secure channel among the communicating entities dynamically. Challenges and trade-offs to the proposed model emerged from the acceptable levels of security that were demanded by the communicating nodes and the preservation of scanty energy levels of these nodes for successful network operations. For any key management approach to be highly successful, it should include nodes in a recurrent manner paving the way for the network to cope-up with security and survivability issues. The key management approach proposed by the authors took into account of the similarities and differences between the communicating nodes. The authors had proposed their key management approach in a more elaborate manner by including several constraints. Key management techniques in wireless sensor networks increase the confidence level of users by maintaining the integrity and authenticity of the exchanged information. Recent advances in the electronics and computer technology had increased the complexity of key management techniques in the wireless sensor networks. The traditional key management techniques suffer huge set back due to lack of resources that has a negative impact on their scalability factor. Manikandan G et al [15] had proposed an optimal cluster based key management system (OC-KMS) for wireless sensor networks. As a part of the proposed approach the authors had utilized the JAYA trust model for designing a modified animal diaspora (MAD) optimization algorithm and selecting the cluster head (CH) as well. This results in energy efficient clustering. The authors had designed les signcryption algorithm certificate for generating and distributing the public and private keys for each node in the sensor network. The proposed approach overcomes a number of attacks at the network layer level without any performance degradation. The proposed optimization approach enhances the trust and security level and energy consumption level of each node as well as the transmitted information in the network. The certificate less signncryption algorithm enhances the key management approach by consuming less energy, maximizing the network life time and overcoming the network layer attacks. Manikandan G et al[16] had observed that the property exhibited by the wireless sensor nodes of entering and leaving the network at their will gave rise to malicious node entry into the network, making the entire network vulnerable to various types of attacks. An active attack of such type could be the jamming type of attack where the transmitted data gets corrupted. A dynamic key management technique had been proposed by the authors where the transmitted message hops from channel to channel during its transmit from the source to destination node. Such hopping of channels reduces the likelihood of attacks as data is made to travel on any channel at any specific point of time only for a small duration. The transmitting nodes and their corresponding receivers jointly generate a pseudo-random sequence that is made known none other than them. The generated random sequence contains all the required information regarding channel hopping and their respective orders. This sequence is further confirmed between the sender and the receiver by exchanging a secret key string between them after which they begin exchanging the actual data. The secret string exchanged between the sender and receiver by looking into various parameters like mean value, tolerance level, quantization function.

V. PROBLEM IDENTIFICATION

In this work, a novel key generation algorithm has been designed by applying channel response technique for wireless sensor networks. Every pair of nodes that engage in communication generate a channel hopping sequence based on Leap and Stop technique and the same is exchanged through a channel in a secret manner that is known only to the two participating nodes. The channel sequence exchanged contains details regarding the channels and the time duration for which it would remain active in each round. Upon confirming the channel sequence, each node then collects the channel response on each channel at time interval specified and accordingly generates the secret key.

VI. PROPOSED METHODOLOGY

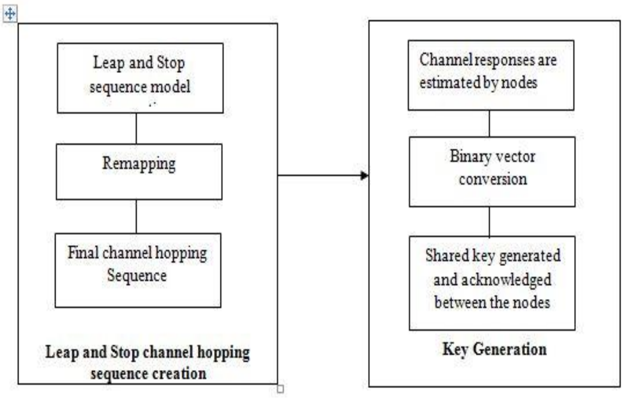

Leap and Stop sequence model
Remapping
Final channel hopping Sequence
Leap and Stop channel hopping sequence creation
Channel responses are estimated by nodes
Binary vector conversion
Shared key generated and acknowledged between the nodes
Key Generation

Fig. 2. Proposed Architecture

A. Leap and Stop channel hopping sequence algorithm

Channel hopping sequence mechanism has been developed to thwart the jamming attack.

The path traversed by data gets changed from one channel to another in a pre-defined sequence. This pre-defined sequence had been shared between the two nodes engaged in communication before any exchange of data. At first, Leap and Stop channel sequence is generated and sample messages containing the complete information on channel sequence gets exchanged between the two nodes involved. The channel sequence generated from the Leap and Stop technique has been described in algorithm given below:

Table-I: Algorithm Notations

Notation	Explanation
N	Number of channels
Q	Smallest prime number
a_0	Non Zero Integer
m_0	Index value
T	Time slot counter
Ch	Channel sequence

Algorithm

The channel hopping sequence is generated in multiple rounds and each round comprises of one Leap model and one Stop model. Users execute the Leap model first followed by the Stop model. Applying their intuition, users profoundly "Leap" on the available channels while carrying out the Leap model and halt at a specific channel in the Stop model.

1. There are three parameters which the user needs to select initially before generating the two models. They are:

   Q – Which is a smallest prime greater than **N** as mentioned in Table-I

   a_0 - a non-zero number selected from [1, $\boldsymbol{N}$]

   m_0–an index selected from [1, $\boldsymbol{N}$].

2. At each round the Leap model and Stop model that follows it extend for 2Qtime slots and Q time slots respectively.

3. This sums up the duration of each round to be equal to 3Qtime slots. User starts the Leap model from an index value of m_0 and continues to hop in the interval range of [1, Q] with the step length measuring to m_0 by performing modulo operations on Q.

4. In the following Stop model, user stays put up on channel a_0.

5. Here, the time slot counter is indicated as t that starts counting from 0. A remapping operation gets executed whenever the channel index m breaches N.

B. Key Generation Using Channel Response

Once the channel sequence is determined, the secret key to be used for guarding the transmission is agreed upon by the sender and receiver. Then the sender and receiver live up to the channel sequence specified for carrying out the data packet/message transmission.

Once the sender and receiver generate their own secret key, they exchange the same for verification purposes so that any misinterpretation during data transmission can be nullified. The secret key generation process and its subsequent verification has been described in the algorithm given below.

Table-II: Notation

Notations	Explanation
X,Y	Nodes
$F'_{YX}(t)$	Estimated Channel Response
$F_{YX}(t)$	Channel Response
$sp(t)$	shape pulse
$n_X(t),n_Y(t)$	noise signals

Algorithm

Let X and Y be the two nodes wanting to carry out a secret communication without involving a key management authority as mentioned in Table-II. Then the following steps need to be performed by these two nodes so that correlated information could be obtained and confirmation of the generated secret key could be made, as summarized in

Step1- A known shape pulse $sp(t)$ is exchanged between the communicating nodes.

Step2–A quasi-stationary environment (where the movement is restricted) needs to be upheld for performing this operation.

Step3- The channel responses are then estimated by the nodes X *and* Y as given below:

$$F'_{YX}(t) = F_{YX}(t) + n_X(t) \qquad (1)$$

$$F'_{XY}(t) = F_{XY}(t) + n_Y(t) \qquad (2)$$

where the estimates of the channel responses $F_{YX}(t)$ and $F_{XY}(t)$ are indicated by $F'_{YX}(t)$ and$F'_{XY}(t)$. Errors in the estimates are denoted by the noise signals $n_X(t)$ and $n_Y(t)$, which can be considered as zero-mean Gaussian noises. A similar true channel responses could be assumed on the basis of reciprocity hypothesis (i.e.$F_{YX}(t) \equiv F_{XY}(t)$)

Step 4 –The adaptive quantization algorithm [18] is used for translating the channel estimates to binary vectors. Long secret keys can be efficiently created use this algorithm by guaranteeing a high key agreement ratio between the authorized users and subsequently reducing the amount of information that could be revealed to attackers.

Step 5 –The presence of measurement noise could give rise to errors in the deduced binary vectors. Hence each node performs an algebraic coding method to correct the dissimilar bits that may be present. This is followed by the generation of a hash for verification purposes between the nodes.

Step 6 –Finally, upon receiving a positive acknowledgement, the shared secret key could be used for initiating a secure communication between the concerned parties.

Step 7 – In contrast, if the nodes do not agree on the same key, the previous steps are repeated till a consensus among them is reached.

Thus by applying the above stated algorithm, a secret key could be successfully generated without getting entangled in to any sort of attacks in the network by any adversary.

VII. SIMULATION RESULTS

A. Simulation parameters

The proposed approach of Key Management system using Channel Response (KMCR) protocol had been simulated using NS2. The MAC layer protocol for WSNs used in the simulation purposes are IEEE 802.15.4. The selected protocol can effectively send notification to the network layer about any significant line breakage. The packet sending rate has been varied in the range of 20, 40, 60, 80 and 100 Kb for the simulation purposes. The chosen area size is 100 metre × 100 metre square region for simulation duration of 60 seconds. The simulated traffic is constant bit rate (CBR). The simulation settings and parameters involved had been summarized in Table- III

Table-III: Simulation Settings

No. of nodes	200
Area	100× 100
MAC	802.15.4
Simulation time	60 sec
Traffic source	CBR
Rate	100 Kb
Propagation	Two ray ground
Antenna	Omni antenna

B. Performance Metrics

The performance of the proposed KMCR(Key Management using Channel Response) protocol had been compared against the Secure Key Generation using Frequency Selective Channels (SKGFSC) protocol [19]. The comparison had been carried out by considering the following parameters:

Average packet delivery ratio: It denotes the ratio of successful number of packets that are delivered out of the total number of packets that are transmitted.

Packet drop: It gives the account of number of packets that are dropped during transit between source and destination.

Energy: Amount of energy needed for transmitting the data

VIII. RESULTS AND ANALYSIS

The simulation results are presented in the next subsequent section.

A. Based on Attackers (Scenario-1)

In the experiment 1 that had been conducted, the number of attackers is varied as 1, 2, 3, 4 and 5 for CBR traffic. The performance of the proposed approach based on the parameters of delivery ratio, packet drop, and energy had been depicted in the figures 3 – 5 for CBR type of traffic and experimental values mentioned in Table-IV to VI. In all these set-ups the attacker count is varied from 1 to 5 for the CBR type of traffic. Comparison in these figures had been carried out between the proposed KMCR approach and SKGFSC protocol. From the figures 3 – 5 it is evident that the proposed KMCR approach provides 45% better delivery ratio, 40% drop in packet count and 5% better energy conservation when compared with the SKGFSC protocol.

Table-IV: Attackers and Packets Drop

Attackers	SKGFSC	KMCR
1	1002	962
2	988	981
3	1201	1061
4	1199	1048
5	1389	1451

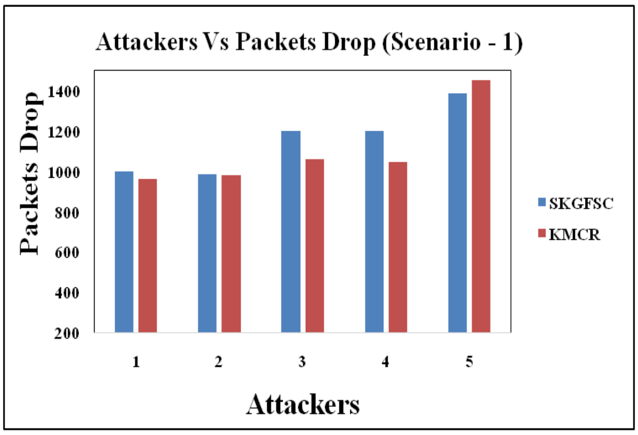


Fig. 3. Attackers Vs Packets Drop

Table-V: Attackers and Delivery Ratio

Attackers	SKGFSC	KMCR
1	0.231	0.462
2	0.296	0.592
3	0.31	0.62
4	0.299	0.598
5	0.358	0.716

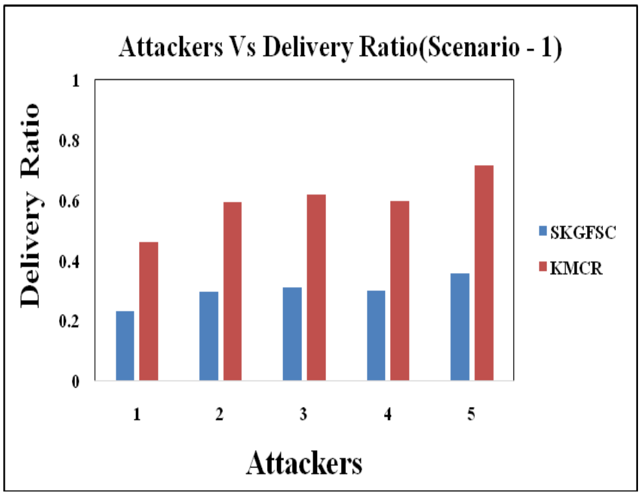


Fig. 4. Attackers Vs Delivery Ratio

Table-VI:Attackers and Energy

Attackers	SKGFSC	KMCR
1	0.332	0.629
2	0.394	0.598
3	0.312	0.542
4	0.386	0.602
5	0.294	0.631

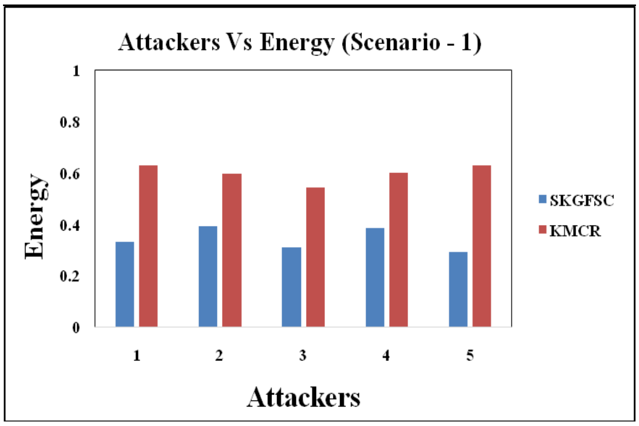


Fig. 5. Attackers Vs Energy

B. Based on Attackers (Scenario-2)

In the experiment 2 that had been conducted, the number of attackers is varied as 1, 2, 3, 4 and 5 for Poisson (exponential) traffic.

Table-VII: Attackers and Packets Drop

Attackers	SKGFSC	KMCR
1	1180	1123
2	1166	1144
3	1379	1234
4	1377	1241
5	1667	1615

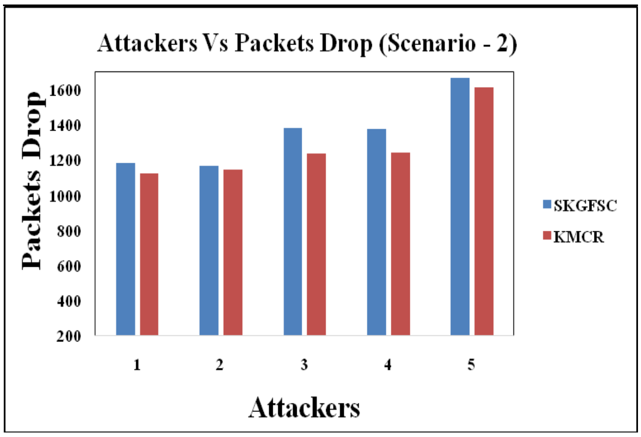


Fig. 6. Attackers Vs Packets Drop

Table -VIII:Attackers and Delivery Ratio

Attackers	SKGFSC	KMCR
1	0.2833	0.477
2	0.2783	0.615
3	0.3193	0.635
4	0.3713	0.656
5	0.3503	0.739

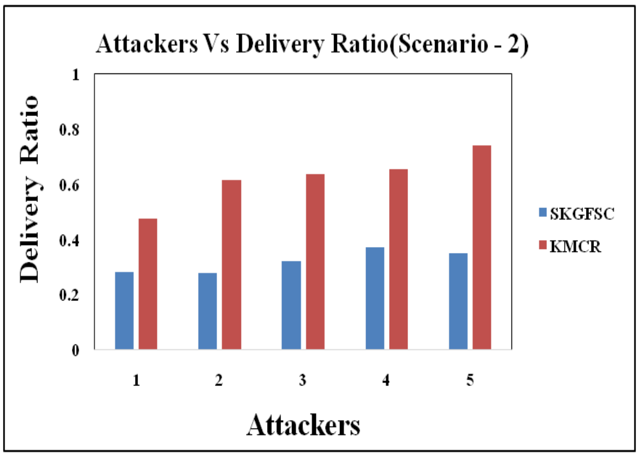


Fig. 7. Attackers Vs Delivery Ratio

Table-IX:Attackers and Energy

Attackers	SKGFSC	KMCR
1	0.418	0.6312
2	0.469	0.5998
3	0.389	0.5431
4	0.462	0.6042
5	0.362	0.6325

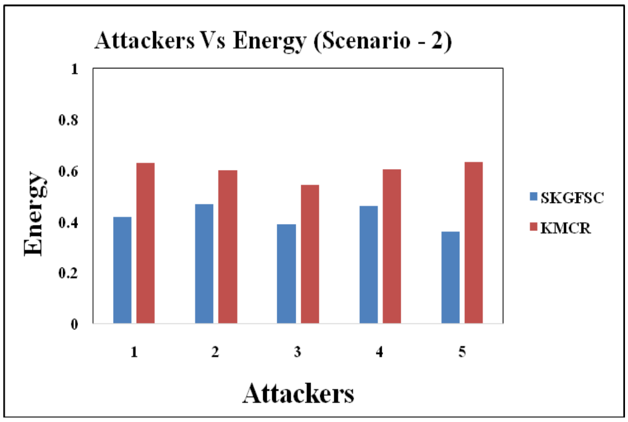


Fig. 8. Attackers Vs Energy

The performance of the proposed approach based on the same parameters of delivery ratio, packet drop, and energy had been depicted in the figures 6 – 8 for exponential traffic (Poisson type). In all these set-ups the attacker count is again varied from 1 to 5 for the Poisson type of traffic and experimental values mentioned in Table-VII to IX.. Comparison in these figures had been carried out between the proposed KMCR approach and SKGFSC protocol. From the figures 6 – 9 it could be inferred that the proposed KMCR approach provides 33% better delivery ratio, 35% drop in packet count and 4% better energy conservation when compared with the SKGFSC protocol.

IX. CONCLUSIONS

The wireless sensor networks are always vulnerable to various types of security attacks. The most common of them is the node capture and data jamming attack. To make the WSN more secure and robust against these attacks, a novel key management approach had been proposed using the channel response technique. A channel sequence had been initially generated by the sender and receiver using the Leap and Stop algorithm. The generated channel sequence is made known only to the sender and receiver. Channel sequence that is shared between the sender and receiver details out the information about the number of channels that would be used for transmitting data in a predefined order. This sequence is followed by the sender and receiver after each of them gets confirmation regarding a secret key that had been generated using the channel response technique. The criteria involved in the generation of secret key include shape pulse, tolerance level, quantization function, noise signals, etc. Once the generated secret key is confirmed by both the parties, the message transmission begins in the specified channel sequence. The proposed KMCR approach had been compared with SKGFSC approach for its efficiency and performance by taking into account of Packet Drop, Packet Delivery Ratio and Energy parameters. Experimental results obtained had proved the supremacy of the proposed KMCR approach.

REFERENCES

1. Akyildiz, I.F., Su, W., Sankarasubramaniam, Y. and Cayirci, E., 2002. “A survey on sensor networks,” IEEE Communications magazine, 40(8), pp.102-114.
2. Pathan, Al-Sakib Khan, Hyung-Woo Lee, and ChoongSeon Hong. “Security in wireless sensor networks: issues and challenges,” Advanced Communication Technology, 2006.ICACT 2006.The 8th International Conference.Vol. 2.IEEE, 2006.
3. Zhang, Xinyang, and Jidong Wang. “An efficient key management scheme in hierarchical wireless sensor networks,” Computing, Communication and Security (ICCCS), 2015 International Conference on. IEEE, 2015
4. Bhaskar, Pranave Kumar, and Alwyn R. Pais. “A Chinese remainder theorem based key management algorithm for hierarchical wireless sensor network,” International Conference on Distributed Computing and Internet Technology. Springer, Cham, 2015.
5. Suganthi, N., and SumathyVembu. “Energy efficient key management scheme for wireless sensor networks,” International Journal of Computers Communications & Control9.1 (2014): 71-78.
6. Gupta, Ankit, and PriyankaAhlawat. “Improved blom key management scheme for wireless sensor network,” Recent Advances and Innovations in Engineering (ICRAIE), 2014. IEEE, 2014.
7. Qin, Zhongyuan, et al. “An efficient identity-based key management scheme for wireless sensor networks using the bloom filter,” Sensors 14.10 (2014): 17937-17951.
8. Kazienko, Juliano F., et al. “SENSORLock: a lightweight key management scheme for wireless sensor networks,” Security and Communication Networks 6.10 (2013): 1198-1210.
9. Du, Dahai, HuagangXiong, and Hailiang Wang. “An efficient key management scheme for wireless sensor networks,” International Journal of Distributed Sensor Networks 8.1(2012): 406254.
10. Zhang, Xing, Jingsha He, and Qian Wei. “EDDK: Energy-efficient distributed deterministic key management for wireless sensor networks,” EURASIP Journal on Wireless Communications and Networking 2011.1 (2011): 765143.
11. Liang, Haijun, and Chao Wang. “An energy efficient dynamic key management scheme based on polynomial and cluster in wireless sensor networks,” Journal of Convergence Information Technology 6.5 (2011): 321-328.
12. Messai, M-L., MakhloufAliouat, and HamidaSeba. “Tree based protocol for key management in wireless sensor networks,” EURASIP Journal on Wireless Communications and Networking 2010.1 (2010): 910695
13. Bechkit, W., Challal, Y., Bouabdallah, A., &Tarokh, V. (2013). A highly scalable key pre-distribution Scheme for wireless sensor networks. IEEE Transaction Wireless Communication, 12(2).
14. Eltoweissy, M., Moharrum, M., &Mukkamala, R. (2006). Dynamic key management in sensor networks.IEEE Communication Magazine, 44(4), 122–130.
15. Manikandan , G. And sakthi, U., 2018. Optimal cluster based key management system using signcryption algorithm for wireless sensor networks. Neural network world, 28(5), pp.433-455.
16. Manikandan, G. And Sakthi, U., 2018. Dynamic key management system using channel hopping in ieee 802.15. 4 wireless sensor networks. International journal of mobile network design and innovation, 8(2), pp.73-79.
17. R.Divya, T. Thirumurugan,”A Novel Dynamic Key Management Scheme Based OnHamming Distance For Wireless Sensor Networks”, Proc. International Conference onComputer, Communication and Electrical Technology-ICCCET 2011, 18th &19th March,2011, pp. 181-185.
18. S. Tmar-Ben Hamida, J.-B.Pierrot, and C. Castelluccia, “An adaptive quantization algorithm for secret key generation using radio channel measurements,” in Proceedings of the 3rd international conference on New technologies, mobility and security, 2009, pp. 59–63.
19. Wilhelm, M., Martinovic, I. and Schmitt, J.B., 2013. Secure key generation in sensor networks based on frequency-selective channels. IEEE Journal on Selected Areas in Communications, 31(9), pp.1779-1790.
20. Manikandan, G., Suresh, K. and Annabel, L.S.P., 2019, November. Performance Analysis of Cluster based Secured Key Management Schemes in WSN. In 2019 International Conference on Smart Systems and Inventive Technology (ICSSIT) (pp. 944-948). IEEE.
21. Manikandan, G. And Sakthi, U., 2018, August. A Comprehensive Survey on Various key Management Schemes in WSN. In 2018 2nd International Conference on I-SMAC (iot in Social, Mobile, Analytics and Cloud)(I-SMAC) I-SMAC (iot in Social, Mobile, Analytics and Cloud)(I-SMAC), 2018 2nd International Conference on (pp. 378-383). IEEE.

AUTHORS PROFILE

Manikandan.G (Manikandan Gunasekar) obtained his Bachelor's degree in Computer Science and Engineering from St.Joseph's College of Engineering, Tamilnadu, India. Then he obtained his Master's degree in Computer Science and Engineering from St.Joseph's College of Engineering, Tamilnadu, India. Currently, he is a research scholar in Sathyabama Institute of Science and Technology, Chennai, India and he is an Assistant Professor at the Department of Information Technology, St.Joseph's College of Engineering, Chennai-119, India. His current research interests are Wireless Sensor Networks, Mobile Networks, Data mining.

Dr.Sakthi.U (Sakthi Ulaganathan) received her Ph.D. Degree from Anna University, Chennai, India. Currently, she is Professor at the Department of Computer Science and Engineering, St.Joseph's Institute of Technology, Tamilnadu, India. She has more than 10 years of teaching experience in Engineering College. She has published more than 20 papers in international conference and Journals. Her current research interests are Grid computing, Data mining, Mobile networks.