Published by :
http://www.ijert.org

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 8 Issue 06, June-2019

An Energy Efficient Secure Communications using Quantum Key Distribution in Wireless Sensor Networks

Anu M R
M.Tech Student, Dept of CSE
LBS Institute of Technology for Women
Trivandrum, India

Sumimol L
Assistant Professor, Dept of CSE
LBS Institute of Technology for Women
Trivandrum, India

***Abstract*— Sensors are most important components used in different electronic appliance. Sensors are of micro size so the power capacity is restricted and the network life time is also very less. Wireless sensor networks comprise of sensor nodes with sensing and communicating ability. Sensor nodes are mainly battery-powered appliance. The censorious feature is to minimize the energy utilization of nodes, so that the network lifetime can be ameliorate to rational times. In military solicitation, it is very arduous to restore or regenerate the battery cell. Therefore, some energy utilization strategies are required to elongate the network lifetime. In this paper, we suggest an energy efficient concord that is simple and workable to contrivance on wireless sensor network. For secure communication Modified AODVQ protocol is used for packet queuing. The enhancement we done in this paper is QKD (Quantum Key Distribution), it is used for secure communication and to recover from the attacks on the networks. We conduct a simulation to examine our work and collate it with the subsist infusion based on the cadent like as intensity of each hops and energy saved while sending messages. Our work shows that the prospective methods are more dynamic and guarded compared to the existing methods.**

Keywords — WSNs; Energy Efficient; Secure Communication; QKD; Network Lifetime; Sensor Nodes.

I.INTRODUCTION

A wireless sensor network is a network repressed of resource-constrained appliances that have the capability of communication and sensing through wireless nodes. The WSN dwell of mini sensor nodes which are repressed of some interspersed capabilities for data sensing, congressing, transforming, but they have finite repository space. The sensor nodes have the pulpit for tracking and observing the network and the pulpit rely on battery. The expense and capacity of sensor nodes rely on the resources such as efficiency, memory, computing speed and transmission capacity for communication.

The most decisive element in sensor node is the battery sewerage. Particularly in the battle field, the node disposing and restoration is very crucial. Therefore, energy performance must maintain in such situation. The nodes that fully drown out the battery capacity are called dead nodes. Many inquisitions are going based on how to enhance the energy performance in WSNs. The researchers bring out contrasting approaches for the enhancement of network lifetime. The performance and the network lifetime of WSN depends on the reliable transmission, energy consumption etc.

The inefficient communication leads to data loss or depletion of packets and thus, the network has to send the same data again and again as far as a successful transmission consummates and therefore leads to bandwidth disuse in the network. In such situations, WSN needed some fault resistance and security mechanism against any data dissemination and snooping. The well experienced adoption of wireless sensor network and computer adaptor may grant a way for snoopers in the network for attack. Thus, leads to the data transmission again and again which causes the utilization of more energy. This leads to the violation of QoS transmission in the network. For overcoming such situations, enhanced security methods must be granted along with the routing protocol. Various methods are developed for the communication of data securely in WSNs. The survey paper shows some research on different secure routing protocols and energy efficient methods which gives improved throughput and enhances the network lifetime in WSNs.

In this work, we introduce an efficient and secure key sharing protocol for WSNs known as Quantum key distribution. The QKD is used as updation in already existing key generation algorithm in [13]. In our work we consider channel as well as data packet, but given more importance on channel. Inside QKD we are updating the cryptographic techniques. Multihop and single hop base communication is carried out in this paper.

The gesture of this paper is formulated as follows: Section II illustrate the work associated to the energy efficiency and secure communication. Section III illustrates the proposed techniques. Section IV illustrates the Quantum key distribution. Section V illustrates the RSA algorithm. Section VI illustrates the result analysis. Section VII concludes the paper.

II. RELATED WORKS

In [1], the author introduced an Improved Distributed Energy Efficient Clustering (I-DEEC) method for increasing the life of a sensor node. This method is correlated with DEEC and EESAA. DEEC (Distributed Energy Efficient Clustering) protocol is used to prefer cluster heads based on halting

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 8 Issue 06, June-2019

energy and evaluate the increase in network lifetime. EESAA (Energy Efficient Sleep Awake Aware) protocol scale down the use of energy and grant security in network lifetime and make effort on pairing while the bystander nodes makes the pair for data transferring and further communication. The proposed technique, I-DEEC implement to establish the energy service in current protocol i.e; DEEC which finds the optimal passage from sender to receiver.

In [2], the author establish an energy management key for both routing layer and MAC layer protocols. First, they go for the pattern of routing protocol which is based on the current IECBR (Improved Energy Efficient Chain Based Routing) technique. In this technique, HBO (Honey Bee Optimization) scheme is used for optimally choosing the nodes. To increase the energy efficiency, they reorganize the MAC protocol according to the dynamic back off algorithm known as improved sensor MAC (IS-MAC). In here, contention window (CW) regulates dynamically in the MAC protocol to attain energy efficiency by knobbing the network load productively.

In [3], the author introduces a multihop energy efficient transmission approach in WSN. The paper presents a system standard for their network. The system standard dwell of multihop clusters of nodes and each cluster dwell of N sensor nodes. The sensor node disclosure of the information in and around the observing field, then it passes on to the cluster head which in turn distribute to the centre of preservation in order to take the proper intervention. The main aim is to explain a recent energy efficient transmission method that grants for decreasing the energy utilization for increasing the lifetime of WSNs. In this study, they estimate that the transmitting signal will properly received only if the signal to noise ratio (SNR) at the receiver is higher than the threshold. Each cluster dwell of one starting node, one target node (CH) and N-2 relays. The relays that are chosen are those that have minimum transmitting energy while managing SNR that is equal to the threshold. Therefore, the proposed technique minimizes the power utilization while correlating with the forthright transmission and the transmission with a single relay.

In [4], the author specify some recent routing protocol that work to obtain efficient routing along with some enhanced method such as ACO (Ant Colony Optimization), ABC (Ant Been Colony, HBO (Honey Bee Optimization). But these methods fizzled to amuse the WSN demand such as energy efficiency and observing the consummation of network under diverse conditions. In this paper author introduced a novel routing protocol related to the existing IECBR (Improved Energy Efficient Chain Based Routing). IECBR adopt the HBO technique for flawless node selection. The HBO scheme is enhanced with uncontrolled localization which is related to the suitable powerful selection algorithm which assures that the not a single empty node's energy in the network is above their threshold. Therefore, the new routing protocol is called Modified HIECBR (MH-IECBR). The result presents that the proposed technique enhances the consummation of network lifetime while correlated with state of art schemes.

In [5], the research targeted on network topology restrictions which promote each node with an efficient power transmittal to boost the network lifetime and strengthen the network connectivity. The goal of WSN topology control is to layout the arrangement of the nodes for the purpose of minimizing the nodes transmission intervention and enhances the throughput for WSN communication.

III. PROPOSED METHODS

The proposed method includes four phases: Pre-deployment phase, Key distribution phase,Post-key distribution phase, and key refreshment phase.

A.Pre-Deployment Phase

Pre-deployment Phase Steps

$\{K_P, K_R\} \longleftarrow RSA_{gen}$

$K_P \overset{def}{=} AK_{sink}$ and $K_R \overset{def}{=} AK_{nodes}$

$Sink\ node := AK_{sink}$ and $Sensor\ nodes := AK_{nodes}$

$K_{local_i} \overset{R}{\longleftarrow} key_{gen}\{0,1\}^{128}, \forall K_{local_i} \in \{0,1\}^{128} \Rightarrow P\left(K_{local_i}\right) = \frac{1}{|\{0,1\}^{128}|}$

$Sensor\ node_i := K_{local_i}$ and $Sink\ node := K_{local_i}$

The Pre-deployment phase uses an Asymmetric algorithm i.e; RSA algorithm for encryption and decryption of cipher text. The pre-deployment phase consists of five steps:

1. Formation of an asymmetric key pair {KP,KR}←RSA*gen*, where RSA*gen* is the RSA key formation algorithm.
2. KP designated as the sink node key, AK*sink*, and KR is designated as the key for the sensor nodes, AKnodes.
3. AKsink is burdened into the sink node, and AKnodes is burdened into the sensor nodes.
4. The formation of a irregular local key for each sensor nodes as follows: Klocali ← keygen$\{0,1\}^{128}$, where keygen$\{0,1\}^{128}$ is a irregular key formation algorithm with a key space of $\{0,1\}^{128}$; the key space is a homogeneous distribution such that ∀Klocali ∈ $\{0,1\}^{128}$, and the feasibility of each key is P(Klocali)= 1 |$\{0,1\}^{128}$|.
5. Klocali is burdened into the complementary sensor nodei as well as the sink nodes.

B. Key Distribution Phase

Key Distribution Phase Steps

Sink node:

$K_{compl} \longleftarrow Ran_{gen}\{0,1\}^{128}, Tag \longleftarrow H\left(K_{compl}\right)$, and $Timestamp\ T$

$C \longleftarrow E_{AK_{sink}}\left(K_{compl} \,||\, Tag \longleftarrow H(K_{compl}) \,||\, T\right)$

$\overset{send}{\Longrightarrow} \left[C \longleftarrow E_{AK_{sink}}(K_{compl} \,||\, Tag \longleftarrow H(K_{compl}) \,||\, T)\right]$

Sensor nodes:

$\overset{recv}{\Longleftarrow} \left[C \longleftarrow E_{AK_{sink}}\left(K_{compl} \,||\, Tag \longleftarrow H(K_{compl}) \,||\, T\right)\right]$

$P \longleftarrow D_{AK_{nodes}}\left(C \longleftarrow E_{AK_{sink}}\left(K_{compl} \,||\, Tag \longleftarrow H(K_{compl}) \,||\, T\right)\right)$

$f_{verify}(T) = \begin{cases} accept, & if\ T \le time\ threhsold \\ reject, & if\ T > time\ threhsold \end{cases}$

$Tag' \longleftarrow H\left(K_{compl}\right)$

$f_{compare}(Tag, Tag') = \begin{cases} accept, & if\ match \\ reject, & if\ dismatch \end{cases}$

$K_{unique_i} = K_{compl} \oplus K_{local_i}$

After disposing the sensor nodes,

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 8 Issue 06, June-2019

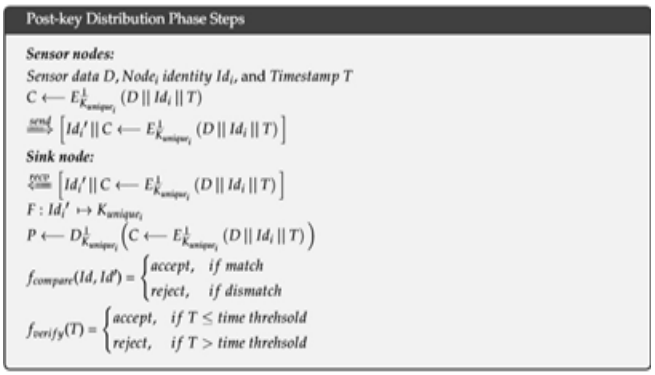
1.The sink node accomplish a irregular complementary key K*compl*←Rangen{0,1}^{128} 2.Computes its hash value Tag ←H(K*compl*).
3.Calculates a timestamp T.
4.After completing this task, the sink node forward the bystander sensor nodes as follows:

$\xrightarrow{send}$[C ← EAKsink (K*compl* ||Tag ←H(*Kcompl*)||T)],
5.These bystander nodes then ahead the cipher to their respective bystander nodes in a multihop way as far as all of the sensor nodes have acquired the cipher,

$\xleftarrow{recv}$[C ←EAKsink (K*compl* || Tag ← H(Kcompl)|| T)],
Here, each nodes are burdened with the asymmetric key AKnodes in the Pre-deployment phase.

6.A sensor node$_i$ can decode the cipher as follows: P←DAKnodes(C←EAKsink(K*compl*||Tag←H(K*compl*)|| T)),
7.And then verifies the timestamp *fverify(T)* based on the predefined threshold, i.e; if timestamp excel the threshold, the sensor node$_i$ deny the cipher.
8.If not, the sensor node$_i$ hashes the complementary key Tag`←H(K*compl*).
9.Correlate it with the received hash *fcompare*(Tag,Tag`) to assure that it has not still received a refitted complementary key K*compl*.
10.If a discrepancy raise, the sensor node$_i$ deny the cipher.
11.If not, the sensor node$_i$ yield its unique key by XORing the complementary key and its local key as follows:
Kuniquei = Kcompl ⊕ Klocali .

C. Post-Key Distribution Phase



After establishing the key distribution phase,

1.The sensor nodes produce the unique keys.

2.When sensor node$_i$ ready to broadcast the data D to the sink node, it adopt its unique key K$_{uniquei}$ to encode the data D, its identity Id$_i$, and a timestamp T.

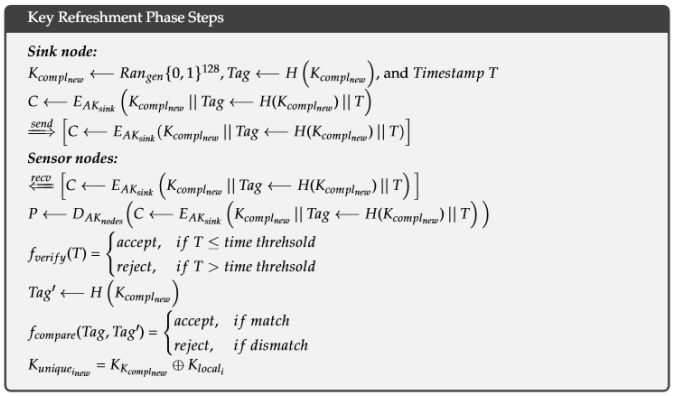
3.Then, it integrate the cipher with another copy if its identity Id$_i$` and forward both to the sink node.These technique is shown below:

$\xrightarrow{send}$[Id$_i$`||C←E$^{\perp}_{K_{uniquei}}$(D|| Id$_i$||T)], where ⊥ is a Probablistics encryption algorithm, since the research is based on key distribution the node$_i$ can able to use several probablistics encryption algorithm.

4.When sink node accept the cipher ie;

$\xleftarrow{recv}$[Id$_i$`||C← E$^{\perp}_{K_{uniquei}}$ (D|| Id$_i$||T)], the sink node uses the concatenated node i.e; Idi` inorder to find the corresponding Kuniquei ie; *F* : *Idi*` → Kuniquei.
5. After finding the Kuniquei, the sink node decode the cipher.
6. Compare the identities *fcompare*(*Id,Id`*) inorder to assure whether the cipher is received from an authorized node and also ensures that appropriate Kuniquei is used.
7. If any match found, then the sink node checks the timestamp T, i.e; *fverify(T)* depend on the predefined threshold.
8. If the timestamp T is less than or equal to threshold value then the sink node recieves the sensor data D, if not deny the data D.

D. *Key Refreshment Phase*



In Key Refreshment Phase Random complementary key is generated and the key refreshment is done based on XOR method. The explanation of above algorithm is as follow:

1.The sink node develop a new Random complementary key i.e; *Kcomplnew←Rangen{0,1}*^{128}, measures the hash value i.e; *Tag←H(Kcomplnew)* and calculate the timestamp T.
2.After generating the random complementary key, using its asymmetric key *AKsink* the sink node encrypts these values.
3.Then transfer the cipher to the bystander nodes i.e;

$\xrightarrow{send}$[C←EAKsink(K*complnew* || Tag←H(K*complnew*)|| T)].
3.As far as, all the sensor nodes receives the cipher

$\xleftarrow{recv}$[C←EAKsink(Kcomplnew||Tag←H(Kcomplnew)||T)],
the neighbors sends the cipher to their bystander nodes in a multihop manner.
4.Since the nodes are burdened with the asymmetric key

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 8 Issue 06, June-2019

AK_{nodes} in the pre deployment phase, the sensor $node_i$ can decode the cipher i.e;

$P \leftarrow D_{Aknodes}(C \leftarrow E_{AKsink}(K_{complnew}||Tag \leftarrow H(K_{complnew})||T))$.

5.Then verifies the timestamp *fverify(T)* depending on the predefined threshold, if T > thresholds the sensor $node_i$ deny the cipher.

6.If not, the node hashes the new complementary key $Tag` \leftarrow H(K_{complnew})$.

7.Compare the value of Tag` with the accepted hash *fcompare(Tag,Tag`)* to assure that it has not yet received a altered new complementary key $K_{complnew}$.

8.If there is dissimilarity, the sensor $node_i$ deny the cipher.

9.If not, it produces its recent unique key by XORing the recent complementary key and its local key i.e;

$K_{unique} = K_{complnew} \oplus K_{locali}$.

IV. QUANTUM KEY DISTRIBUTION

Quantum key distribution is a technique for secure communication that implements a cryptographic protocol that contains components of quantum mechanics. In QKD, it facilitates two parties to share irregular secret key that is only known between them, which is used to encode and decode the messages. Quantum key distribution is also known as quantum cryptography.

The main advantage of QKD is the capability of two communicating users to observe the presence of third party trying to get the details of key.

The Quantum key distribution is only used to distribute and produce a key; it is not used to transfer any message data.

A.QKD'S STRENGTHENS

Quantum key distribution is good method for producing long random keys. Take an example of two person i.e; Alice and Bob communicating through wireless sensor network. A secret key is shared between Alice and Bob for the very first Quantum key exchange to be authenticate. It has been shown that the output of first QKD session is used to authenticate the next QKD session that means this second round is completely secured. Each new QKD is independent of all previously used keys, thus it reduce the number of ways a malefactor attack the system.

The security provided by QKD is future proofed that is even if a cryptographic system is broken at some unspecified time in future, the message sent previously through it remain secure. The unconditional security of QKD is proves that even if an adversary with infinite supplies of time and processing power, the security of QKD cannot be broken.

B. QKD'S WEAKNESSES

The weakness of QKD'S as follows: Quantum channel works for a limited distance; The messages can't be transferred so fast enough to meet the adequate services; quantum equipments are vulnerable to attack; for the support of quantum processing an expensive infrastructure will be needed.

V. RSA ALGORITHM

In pre-deployment phase, RSA algorithm is used for encryption and decryption.RSA is one of the initial public key cryptosystems and is used for secure data communication. In this type of cryptosystem, the encryption key is the open key and the decryption key is the confidential key.

RSA is comparatively slow algorithm, and thus it is less regularly used to directly encode user data. Mostly RSA sends encoded shared keys for symmetric cryptography which can execute large amount of encryption and decryption operations at high speed.

VI. RESULT ANALYSIS

In this section, we will discuss about the energy efficiency while providing secure communication in wireless sensor networks. The project is done in ns3 simulator. Here, we compares the energy consumed based on hops between existing Key generation and QKD-Key generation. The number of nodes we taken is 50. It shows that QKD-Key generations consume less energy compared to existing key generation. The result is shown below:

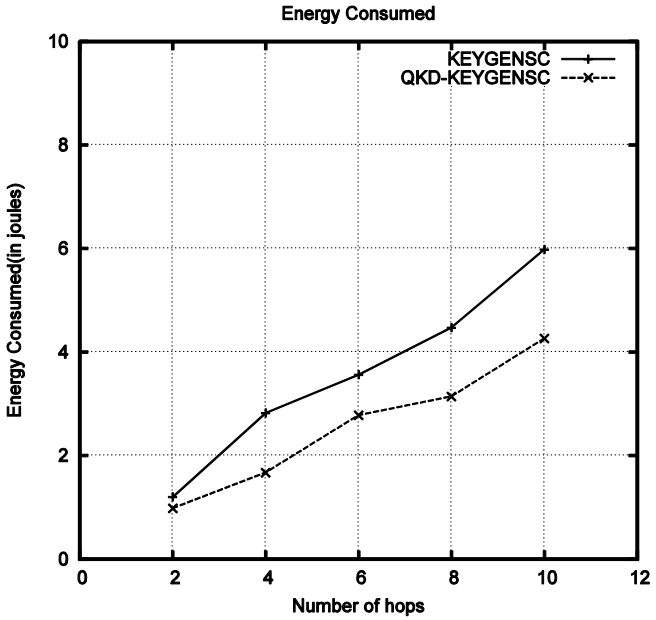


Fig. 1. Energy Hops

The energy consumed according to the number of messages send through the network is compared with the existing key generation. It has shown that the 18% energy has consumed by using the quantum key generation. The graph for energy message is shown below:

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 8 Issue 06, June-2019

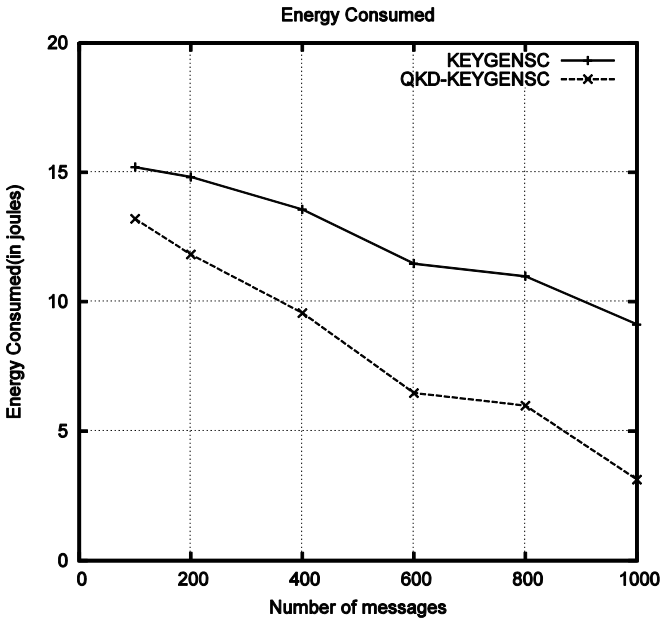


Fig. 2 . Energy Messages

VII. CONCLUSION

In this work, we implemented a practical key distribution technique called Quantum Key Distribution (QKD). This technique is used for secure communication. While using this technique the communication become more secure and the jamming and brute force attacks are able to overcome. The RSA algorithm is used in the Pre-deployment phase for encryption and decryption of cipher text. The key refreshment is done based on the XOR method. The advantage found while using QKD was the number of key generation become less in the network and the connectivity of the link become very high. Since, the time taken for key generation is less thus reduces the energy consumption. The inclusive outcome shows that the suggested protocol enhances its security and thereby reduces the energy consumption.

REFERENCES

[1] M. Young, The Techincal Writers Handbook. Mill Valley, CA: University Science, 1989.
[2] J. U. Duncombe, “Infrared navigation—Part I: An assessment of feasibility (Periodical style),” IJREAM Trans. Electron Devices, vol. ED-11, pp. 34–39, Jan. 1959.
[3] S. Chen, B. Mulgrew, and P. M. Grant, “A clustering technique for digital communications channel equalization using radial basis function networks,” IJREAM Trans. Neural Networks, vol. 4, pp. 570–578, Jul. 1993.
[4] R. W. Lucky, “Automatic equalization for digital communication,” Bell Syst. Tech. J., vol. 44, no. 4, pp. 547–588, Apr. 1965.
[5] S. P. Bingulac, “On the compatibility of adaptive controllers (Published Conference Proceedings style),” in Proc. 4th Annu. Allerton Conf. Circuits and Systems Theory, New York, 1994, pp. 8–16.
[6] G. R. Faulhaber, “Design of service systems with priority reservation,” in Conf. Rec. 1995 IJREAM Int. Conf. Communications, pp. 3–8.
[7] W. D. Doyle, “Magnetization reversal in films with biaxial anisotropy,” in 1987 Proc. INTERMAG Conf., pp. 2.2-1–2.2-6.
[8] G. W. Juette and L. E. Zeffanella, “Radio noise currents n short sections on bundle conductors (Presented Conference Paper style),” presented at the IJREAM Summer power Meeting, Dallas, TX, Jun. 22–27, 1990, Paper 90 SM 690-0 PWRS.
[9] J. G. Kreifeldt, “An analysis of surface-detected EMG as an amplitude-modulated noise,” presented at the 1989 Int. Conf. Medicine and Biological Engineering, Chicago, IL.
[10] J. Williams, “Narrow-band analyzer (Thesis or Dissertation style),” Ph.D. dissertation, Dept. Elect. Eng., Harvard Univ., Cambridge, MA, 1993.