Indonesian Journal of Electrical Engineering and Computer Science
Vol. 15, No. 1, July 2019, pp. 443~450
ISSN: 2502-4752, DOI: 10.11591/ijeecs.v15.i1.pp443-450

Light weight authentication protocol for WSN using ECC and hexagonal numbers

Noel Toy, Senthilnathan T
Department of Computer Science, Christ University, India

Article Info

Article history:

Received Dec 15, 2018
Revised Jan 21, 2019
Accepted Feb 28, 2019

Keywords:

Elliptic curve cryptography (ECC)
Hexagonal numbers
WSN

ABSTRACT

Wireless Sensor Network (WSN) is a spatially distributed network. It contains many numbers of distributed, self-directed, small, battery powered devices called sensor nodes or motes. In recent years the deployment of WSN in various application domains are growing in a rapid pace as with the upcoming boom of Internet of Things (IoT) and Internet of Everything (IoE). However, the effectiveness of the WSN deployment is restricted due to the constrained computation and power source. Hence, many researchers have been proposing new approaches and models to improve the efficiency of the domain specific WSN deployment procedures. Though, many research communities addressing various issues in WSN deployment, still the privacy and security of such networks are susceptible to various network attacks. Thus, it is necessary to practice different models for authentication and privacy preservation in a highly dynamic resource constrained WSN environment to realize the effectiveness and efficiency of the deployment. Hence, this paper addressing an authentication scheme that can reduce energy consumption without compromising on security and privacy. In order to provide a light weight authentication mechanism, this paper proposing an authentication mechanism for WSN deployment by combining the features of Elliptic Curve Cryptography (ECC) and Hexagonal numbers. The feature of ECC is used to reduce the key size and the effectiveness of generating hexagonal numbers is used for minimizing the energy consumption in a resource constrained WSN environment. The results of the proposed approach are evaluated with the different authentication models and the results were indicating that the proposed approach can perform better than the other approaches.

Copyright © 2019 Institute of Advanced Engineering and Science.
All rights reserved.

Corresponding Author:

Noel Toy,
Department of Computer Science,
Christ University, India.
Email: noel.toy@cs.christuniversity.in

1. INTRODUCTION

In recent years, the usage of Wireless Sensor Network (WSN) is the quickly developing innovation in all the application domains. However, security and protection are still to a great extent disregarded, since they are deployed in a resource constrained environment [1]. The data communicated via sensor nodes are vital such as in WSN implemented in tactical networks [2] where the data cannot be eavesdropped by any intruder as it may cause adverse effect. Moreover, the base station must have the capacity to guarantee that the received message was sent by an authorized sensor node and not changed while exchanging [3]. Also, the authenticity and integrity of messages received by base station incredibly impact final outcomes [4].

Ongoing exploration activities in the field of LoWPAN means to incorporate sensors and actuators into traditional IP networks using IPv6 over LoWPAN (6LoWPAN) [5]. 6LoWPAN in reality empowers the combination of smart objects into the general Internet, around the meaning of the Internet of Things (IoT).

In such coming about situation the nearness of billions of objects brings extra issues such as addressing, manageability, scalability, security, privacy, secure mobility and robustness. Therefore, a proficient upgrade of the Internet design and the definition of new protocols are required to adapt to the above difficulties later on in the Internet. In fact, several projects from industrial and international cooperation are being completed to characterize the future internet design which would solve the constraints of the present design counting security, mobility and interoperability for the heterogeneity of network [6]. Most of the times the Wireless sensor network (WSN) are deployed in environments where direct human intervention is minimal or not even possible. Hence remote authorization is mandatory in such situations, through remote authorization the users can gain access to the sensor node and to collect the data. The sensor nodes will sense the data and information from the environment. Some of the data are labeled as classified which will be available only for specific nodes. It is imperative that the original data sent should not be falsified, as it will lead to a false conclusion. Hence, to tackle out all the issues there should be an authentication mechanism in WSN. Because of the resource constrained nature of sensor nodes, it is important to design a secure, effective and light weight authentication and key agreement scheme [7]. The security of conventional user authentication is in view of passwords or cryptographic secret keys [8]. But the problem with password is that it can be easily guessed also storing these keys in a node is a tedious task.

Although the most recent techniques to enhance the security paradigm in WSN networking environments are found efficient in securing the transmitted data packets still there exists a trade-off in between safety and energy consumption where most of the routing based and optimization-based techniques lacks computational efficiency thus it generates power consumption overhead in overall systems [9]. Here comes the challenge of making a security scheme that will work well in resource-constrained environment without compromising any security factors. In response to these challenges, this paper proposing a new authentication and key exchange scheme for the IP-Based Wireless Sensor Networks which reduces the computational overhead of sensor nodes and produces strong authentication. The scheme uses ECC algorithm with Hexagonal Number Series to ensure the effective authentication. The main goal of this work is to reduce communication and computation overheads while achieving strong and secure authentication scheme for wireless sensor networks. Also, the proposed scheme can prevent most of the attacks on WSN.

2. RELATED WORKS

In the literature focus has been given to different existing mechanism that are used of secure authentication in WSN, these mechanisms include different cipher techniques such as block cipher and variations of public key crypto systems. Even though these mechanisms are modified to suite the resource limited environment, still factors such as large packet size effects the overall performance of the 6LoWPAN network and these networks are connected to Internet. The distribution of public keys is a tedious task when the communication is happening between multiple networks. Therefore, existing schemes should be fine-tuned to yield better authentication mechanism for WSN.

Sarmad Ullah Khana has proposed scheme that takes help of ECC algorithm and random numbers for authentication and key exchange in IP-enabled WSN. Since the scheme uses ECC algorithm the key size is comparatively small as compared with another asymmetric cryptographic algorithm such RSA [10]. Even though this scheme is good for the IoT scenario, the random number generator requires more computational power which not desirable.

Jara has proposed a scheme which securely take care of handoffs in 6LoWPAN networks. ID/Locator split architecture has been used for effective authentication. The intended scheme is a combination of Return Routability with Diffie-Hellman Key exchange and ECC with some more modification as it is meant for WSN [11]. The model effectively deals with some of the renowned attacks such as DoS attack and flooding attack. AVISPA tool was used to implement and verify the scheme.

Qing Chang has proposed an authentication protocol which works in node level. The scheme is based on ECC algorithm. The underlying assumption of the proposed mechanism lies on the difficulty in solving elliptic curve discrete logarithm problem (ECDPL) [12]. The presented authentication mechanism stores the private key within the node itself with makes the scheme vulnerable to node compromise attacks.

For cluster based WSN Arazi has introduced a group key generation method base on the ECC algorithm. The scheme uses an algebraic approach where it divides the key generation process [13]. This will help in reducing the computational by distributing the load over nearby nodes. The scheme reduces the execution as well as balances the consumption of power.

An authentication and key distribution mechanism for diverse WSN has been formulated by Khan. The presented scheme reduces the communication overheads and memory cost [14]. The result for the

simulation is promising which shows a good connectivity and with stand with node capture attack at the same time keeping the cost of energy as minimal as possible.

An authentication scheme has been proposed by Holohan which uses virtual certification authorities for signing the public key certificates [15]. The virtual certification authority will be signing some certificates randomly. The nodes should communicate with the virtual certification authority for getting certificate of another node. This mechanism produces a huge communication overhead as it will be communicating with virtual certification authority frequently. The main disadvantage of this is that communication overhead is more when a virtual certification authority does not have a valid certificate for the node.

A Non-Interactive Zero Knowledge Protocol (NIZKP) [16] for authentication based on ECC algorithm has been proposed by Teyi Yann Cedric Lawson. The protocol is mainly intended for IoT based networks. The authentication includes two parties namely prover and verifier, since the protocol works on zero knowledge concept the prover needs to prove that it holds some knowledge to the verifier without sharing it. Once the verifier verifies then the authentication is successful. Authors conducted a real-world performance comparison of NIZKP and Elliptic Curve Diffie-Hellmann (ECDH) was done using Raspberry Pi 3B model and the results were better than ECDH in terms of energy consumption.

Based on the background studies, it is evident that the effective usage of the resources lies on the appropriate cryptographic approaches and authentication mechanisms. Hence, In the proposed work the combination of ECC and Hexagonal numbers were evaluated. In the subsequent section theoretical study of the ECC mechanism and Hexagonal numbers were discussed.

3. RESEARCH METHOD

The proposed authentication scheme is intended for conventional IP-enabled wireless sensor network which works based on the IPV6 LoWPAN i.e. IEEE 802.15.4. The number of nodes in the network varies depending on the number of nodes connected to the network. The number of nodes cannot be predicted hence usage of pre-distributed key system will not appropriate for this scenario as it will take more memory which not desirable. Beside the nodes can move around and may leave the current network and land in another network. Therefore, a new approach is presented here which is grounded on ECC and hexagonal numbers.

General Elliptic Curve Cryptography (ECC): The algebraic structure of elliptic curves over finite fields can be used as a public-key cryptography which is known as Elliptic Curve Cryptography (ECC). The main advantage of ECC is that it provides high security with a minimal key size which is handy in WSN. ECC can be used for key agreement, digital signature, pseudo-random generator etc. ECC can also be used for encryption.

The equation for Elliptic curve is given as: $y^3 + ax + b$

Hexagonal Numbers: A hexagonal number is a figurate number. Hexagonal numbers are sometimes called "*cornered hexagonal numbers*". The k^{th} hexagonal number will be the number of points in a hexagon with *k* regularly spaced points on a side [17].

The following formula can be used to find out k^{th} hexagonal number.

$$h_k = k\,(2k - 1)$$

Some of the hexagonal numbers are 1, 6, 15, 28 etc. Hexagonal number is a subset triangular number, which means hexagonal number have properties of triangular number but the opposite is not true. Only the numbers 1, 3, 6 or 9 can become the digital root in base 10 of a hexagonal number, which is quite similar to triangular numbers. In 1830 Adrien-Marie Legendre have proven that integers that exceeds 1791 can be represented in terms of at maximum of four numbers, where those numbers follow hexagonal number equation.

The number of nodes in the network is enormous and the nodes are mobile as they are expected to move in and out of the network. Due to this there will be frequent key establishments, in such a scenario ECC is handy as the key size is much smaller compare to some of the other conventional encryption techniques such as RSA and AES. Even though the size of key is smaller in ECC, it doesn't compromise on the security. With shorter key size, key establishment packet size will be reduced and which in turns reduces the energy consumption of the network.

In the proposed scheme, the new network effortlessly verifies the node which is coming to the network by producing its authentication key as an alternative of acquiring the node's previous network's authentication key from the node itself. This will reduce the communication and packet exchange which in turn saves the energy. Also, the proposed system eliminates the introduction of any new security flaws.

The Figure 1 depicts the network reference model which consider two different networks connected via edge routers. The entities present in network reference model are sensor nodes and edge routers. The main responsibility of sensor node is to collect the data from environment and to send it to appropriate destination node. The edge routers perform various security related tasks such as assigning hexagonal number hence it is called as Network Security Manager. All the communication happening between two sensor nodes, which belongs to two different networks will be channelized by the Network Security Manager in other words Network Security Manager acts as a bridge between two different networks.

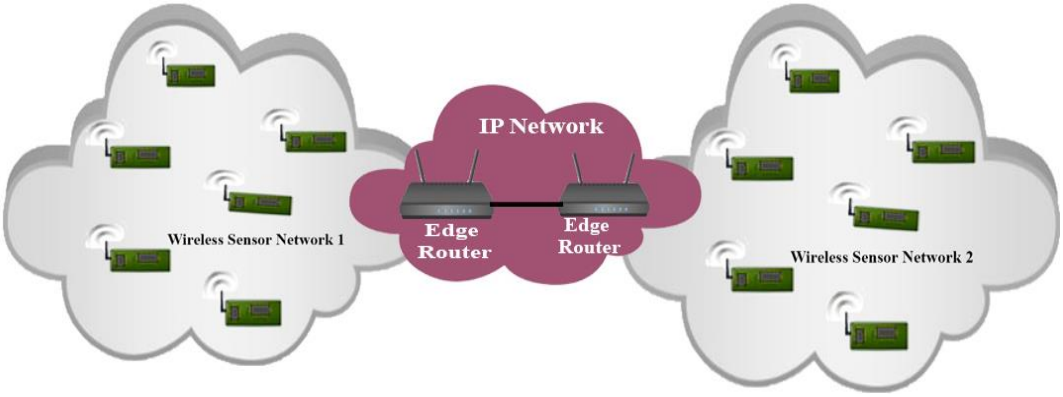

Figure 1. Network reference model which consider two different networks connected via edge routers

Different Phases in the proposed work includes:
- Offline Key Assignment Phase
- Authentication Phase
- Private Key Generation Phase

Offline Key Assignment Phase

Each node is assigned with some important components offline which will be further used for the authentication mechanism. The pre-stored components are used generate authentication key which will help the nodes in verifying each other. Also, these components will help in creating both public and private keys which will aid in securing the communication between two nodes by encrypting and decrypting messages by using the generated key pair. Important steps in this phase includes:

a) Network Security Manager will designate a hexagonal number to all the nodes in the network, this assignment is done after the registration of the node.
b) The proposed system has two parts for the public key which includes network share and node share. In this node share will be designate to the node. Whereas the network share will be generated and stored in the Network Security Manager, that is associated with the node.
c) Source and destination IP address are used for creating the elliptic curve, which will be further used for secure communication between two nodes.
d) G_e and G_n are group generators which are associated with every node and a network respectively.

The Figure 2 depicts the various dialogue exchanges happening between the registering sensor node and its network security manager.

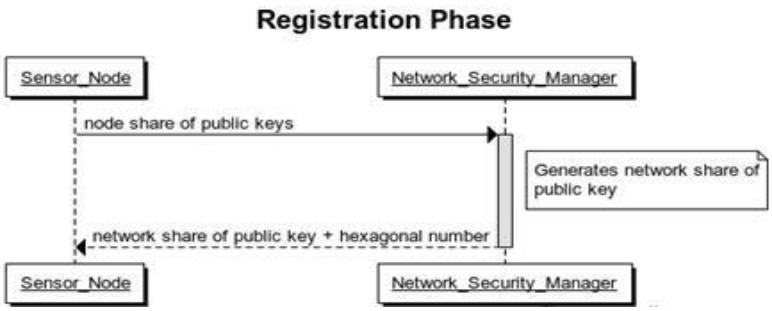

Figure 2. Various dialogue

Authentication Phase

The first and vital step in the proposed scheme. Which provides trust factor for the network entities that are taking part in the communication. The main aim of this phase is to verify the identity of the nodes that are taking part in the communication. This will help in preventing the access of adversary to the network resources and also not to exploit other possible network vulnerabilities. Here, as we specified earlier the in Figure 3 the network scenario consist of two different networks, all the further detailing assumes that sender node and receiver node belongs to two different networks and also depicts how these nodes authenticates each other.

The proposed scheme will be using ECC grounded online key generation. Since the scheme uses ECC, the memory requirement is minimal. The key associated with a node should be revoked when the node is compromised by the adversary, this can be done effortlessly with the help of ECC. All the nodes in the network is designated with a prime number which is denoted as '*p*'. This prime number will be used while generating the private key. The important fact that should be noted here is that, every node will be having one public key and this public key will be used by all the destination node for the verifying the source node. Following formula is used to compute the public key of the node:

$$\boldsymbol{Public\ Key\ = f\{Node\ S\ hare, Network\ S\ hare\}}\ \textbf{(1)}\ [9, .\ (1)]$$

The network share helps in identifying the network to which the node belongs and that can be verified against the network that the node claims. Following equations are used to formulate node and network share respectively.

$$\boldsymbol{Node\ Share = S = IPNetwork\ .\ c\ .\ G_{SN}\ mod\ P_{SN}}\ \textbf{(2)}\ [9, (2)]$$
$$\boldsymbol{Network\ Share = T = S\ .\ G_{N}\ mod\ P_{N}}\ \textbf{(3)}\ [9, (3)]$$
$$\boldsymbol{Public\ Key = Node\ Share \oplus Network\ Share\ mod\ P}\ \textbf{(4)}\ [9, (4)]$$

In the (2) and (3) prime number and group generator associated with network security manager are represented as P_N, G_N respectively and with respect to sensor node it is represented as P_{SN}, $G_{SN.}$ The point on the curve is represented as 'c' and 'P' depicts the field generator and 'P' should be prime.

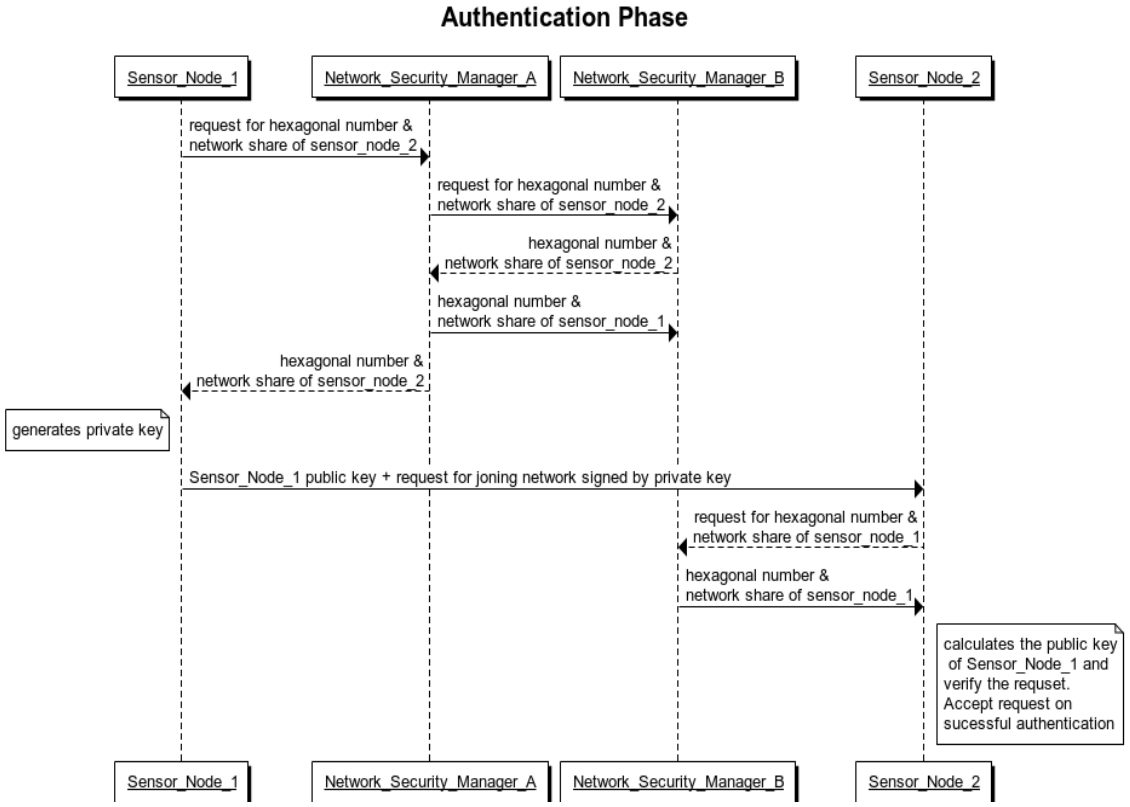

Figure 3. Dialogue exchange between various components in the above specified network scenario

The authentication phase starts when the source sensor node requests to communicate with the destination sensor node which is connected with another network. The communication between source and destination node will take place via network security manager. Figure 3 depicts the dialogue exchange between various components in the above specified network scenario. The network security manager of source node will receive a request packet from the source node. The packet will contain request for hexagonal number and network share that is associated with destination node. The network security manager will connect with the destination network security manager and gets the required parameters. The source network security manager will also share the hexagonal number and node share of the source node. Once the hexagonal number and node share is received the source will calculate the private key and signs a request to message to the destination. When destination node receives the request, it will request the hexagonal number and network share of source to its network security manager. Once destination gets the required parameter then it will compute the public key of the source node and will validate the request to join message sent by source node, upon successful validation the destination will follows the same procedure so that source will be authenticate the destination.

Decryption Key (Private Key) Generation Phase

For the authentication between two different nodes that belongs to two different networks the proposed scheme will generate two private keys i.e. for both source node (SN_1) and destination node (SN_2). This private key can only be used for the authentication between SN_1 and SN_2. If node SN_1 needs to communicate with another node other than SN_2 then SN_1 will generate another private key by using the hexagonal number that is associated with the new destination node. The private key is formulated by using following equation:

$$\boldsymbol{Private\ Key} = (\boldsymbol{Public\ Key} \oplus \boldsymbol{Hexagonal\ Number})^{-1} \boldsymbol{mod\ PSN\ (5)}$$

Where the public key belongs to the source node and the hexagonal number belongs to the destination node. The following sections discusses the evaluation of the proposed work described in this section.

4. RESULTS AND DISCUSSION

The proposed scheme has been successfully implemented and tested with the help of Cooja simulator which is a part of Contiki network operating system that is completely build on Linux kernel. The simulator is mainly intended for the simulation of IoT based IPV6 networks and contains various tools for creating and analyzing various large- and small-scale networks. The simulation results were analyzed and compared with existing schemes and the results were quite satisfying.

Simulation Environment

Table 1 depicts the simulation environment used for proposed scheme which is implemented in the Cooja simulator. The proposed scheme was evaluated on the basis of total energy consumed during packet exchange for key establishment. The power consumption of the sensor node is calculated using the following formula.

Table 1. The Simulation Environment

Parameter	Value
Simulator	Cooja Simulator in Contiki OS
Mote Name	Tmote Sky
RAM	10 kB
ROM	48 kB
Antenna Range	50m(indoors) and 125m(outdoors)
Battery Capacity	2900 mAh
Voltage	3.0 Volt
No. of Nodes	50
No. of Networks	2
Network Type	IEEE 802.15.4/LoWPAN

$$Power(mW) = \frac{rxon}{cpu+lpm} \times 20mA \times 3v \ (\mathbf{6})$$

Where '*rxon*' is the time when the sensor node was in receiver mode, '*cpu'* refers to the active mode time of the CPU and '*lpm*' refers to the time that CPU spent in low-power mode. 20mA is the pre-measured current given by datasheet. 3volts is the operational voltage of mote.

Figure 4 depicts the power consumed by the network for key generation and signature when there are 4, 8, 12 and 20 nodes respectively with two different authentication schemes. The comparison is made between the proposed system and the existing scheme i.e. Elliptical Curve Digital Signature Algorithm (ECDSA). X axis of the graph represent the number of nodes whereas the Y axis represent the power in milliwatts (mW). The graph shows that the proposed scheme with hexagonal numbers takes less power compared to ECDSA.

It also depicts the time consumed by the network for key generation when there are 4, 8, 12 and 20 nodes respectively with two different authentication schemes. The comparison is made between the proposed system and ECC with random number-based authentication [10, p. 1]. From the graph, it is noticed that the proposed scheme takes less time, which is very much important for resource constrained environment, when compared with one of the existing approaches.

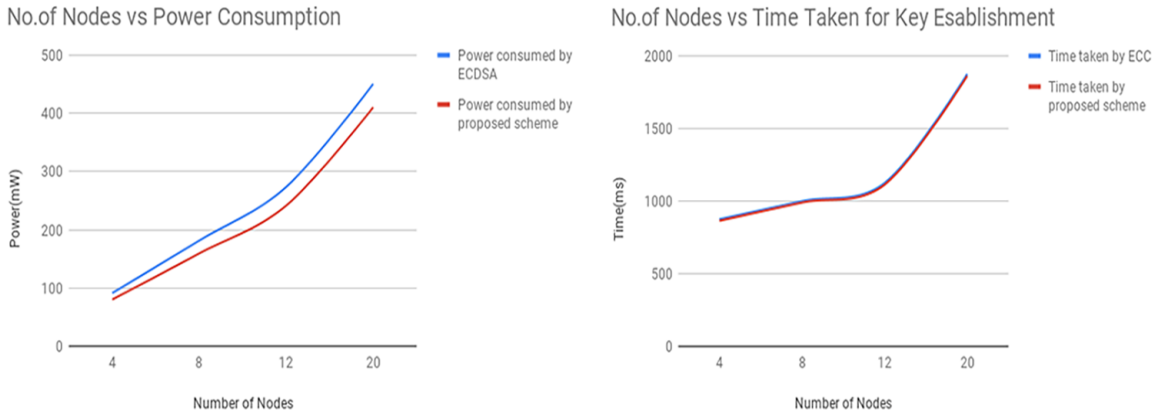

Figure 4. Power consumed by the network for key generation

5. CONCLUSION AND FUTURE WORK

The proposed study formulated a novel model of security paradigm that enhances the energy efficiency without compromising the security. The scheme uses ECC algorithm with Hexagonal number series to generate keys which will be used for authentication. The evaluation of simulation results shows that the proposed scheme is better than many of the existing scheme. Moreover, the study ensures that the scheme can be further extended in future to evaluate the performance in real world rather than using simulators. Also, energy optimized routing can be incorporated in the future to yield a better energy efficient routing protocol for WSN.

REFERENCES

[1] A. Abduvaliev, S. Lee and Y.-K. Lee, "Simple Hash Based Message Authentication Scheme for Wireless Sensor Networks," in *9th International Symposium on Communications and Information Technology*, Korea, 2009.

[2] Shengjun Su, Shuozhong Wang, "A simple monitoring network system of Wireless," *Buletin Teknik Elektro dan Informatika*, vol. 1, no. 4, pp. 251-254, 2012.

[3] I. Akyildiz, Y. S. W. Sankarasubramaniam and E. Cayirci, "A Survey on Sensor Networks," *IEEE Communications Magazine*, vol. 40, no. 8, pp. 102-116, 2002.

[4] I. Akyildiz and I. Kasimoglu, "Wireless sensor and actor networks:research challenges," *Ad Hoc Networks 2(4)*, pp. 351- 367, 2004.

[5] A. Jara, L. Marin, A. Skarmeta, D. Singh, G. Bakul and KimDaeyeoul, "Secure Mobility Management Scheme for 6LoWPAN," *Innovative Mobile and Internet Services in Ubiquitous Computing (IMIS)*, pp. 310-315, 30-02 June-July 2011.

[6] Tseng Huei-Ru, Jan Rong-Hong and Yang Wuu, "An Improved Dynamic User Authentication Scheme for Wireless Sensor Networks," in *IEEE Global Communications Conference(GLOBECOM 2007, Washington, DC, USA)*, Washington, 2007.

[7] Kaiping Xue, Changsha Ma, Peilin Hong and Rong Ding, "A temporal-credential-basedmutualauthenticationandkey agreement schemeforwirelesssensornetworks," *Journal of Network and Computer Applications*, vol. 36, no. 1, pp. 316-323, January 2013.

[8] M. Hwang and C. Liu, "Authenticated encryption schemes: Current status and key issues," *International Journal of Network Security*, vol. 1, no. 2, pp. 61-73, 2005.

[9] Manjunath B. E., P. V. Rao, "Balancing Trade-off between Data Security and Energy Model for Wireless Sensor Network," *International Journal of Electrical and Computer Engineering*, vol. 8, no. 2, pp. 1048-1055, 2018.
[10] Sarmad Ullah Khana, Claudio Pastroneb, Luciano Lavagnoa, Maurizio A.Spiritob, "An Authentication and Key Establishment Scheme for the IP-Based Wireless Sensor Networks," *Procedia Computer Science*, vol. 10, pp. 1039-1045, 2012.
[11] A.J. Jara, L. Marin, A.F.G. Skarmeta, D. Singh, G. Bakul, Daeyeoul Kim, "Mobility Modeling and Security Validation of a Mobility Management Scheme Based on ECC for IP-based Wireless Sensor Networks (6LoWPAN)," in *nnovative Mobile and Internet Services in Ubiquitous Computing (IMIS), 2011 Fifth International Conference*, 2011.
[12] Qing Chang, Yong-ping Zhang, Lin-lin Qin, "A node authentication protocol based on ECC in WSN," in *Computer Design and Applications*, 2010.
[13] O. Arazi, H. Qi, "Self-certified group key generation for ad hoc clusters in wireless sensor networks," Computer Communications and Networks," in *Computer Communications and Networks, 2005. ICCCN 2005. Proceedings. 14th International Conference*, 2005.
[14] S.U. Khan, C. Pastrone, L. Lavagno, M.A. Spirito, "An energy and memory-efficient key management scheme for mobile heterogeneous sensor networks," in *Risk and Security of Internet and Systems (CRiSIS), 2011 6th International Conference*, 2011.
[15] E. Holohan, M. Schukat, "Authentication Using Virtual Certificate Authorities: A New Security Paradigm for Wireless Sensor Networks," in *Network Computing and Applications (NCA), 2010 9th IEEE International Symposium*, 2010.
[16] Teyi Yann Cedric Lawson, Senthilnathan T, "Effectiveness of the NIZKP Protocol for Authentication in IoT Environment," *International Journal of Engineering & Technology*, vol. 7, no. 6, pp. 231-235, 2018.
[17] M.A. Gopalan, P. Jayakumar, "On hexagonal numbers," *International Journal Acta Ciencia Indica*, vol. 32, no. 1, pp. 1217-1219, 2006.