An Efficient and Novel Key Establishment Scheme for Internet Enabled Wireless Sensor Network in the Context of IOT

Karthikeyan.M
PG Scholar, Department of CSE (PG)
Sri Ramakrishna Engineering College, Coimbatore.

J.Selvakumar, Ph.D
Professor, Department of software Engineering (PG)
Sri Ramakrishna Engineering College, Coimbatore.

Amal Twinkle Mathew,
PG Scholar, Department of CSE (PG)
Sri Ramakrishna Engineering College, Coimbatore.

ABSTRACT

Wireless sensor networks (WSN) behave as a digital skin, providing a virtual layer where the information about the physical world can be accessed by any computational system. As a result, they are an invaluable resource for realizing the vision of the Internet of Things (IoT). Many applications of sensor networks require secure communication. Thus establishing a secure channel between any two sensor-nodes in WSNs/IESNs is important for many applications, such as secure data exchange, secure data aggregation, and secure routing. In this paper, first we show why existing three party key establishment schemes cannot be easily applied to IESN. Second we propose an extension of traditional three-party key establishment schemes (such as SNEP, BBF and OR). The method provides DoS and Sybil attack resistance and benefits from low communication cost, independence of prior sensor deployment knowledge and support for node mobility. In comparison to the previous well-known three-party schemes, our extension not only fixes DoS vulnerability, but also provides some other advantages such as significant efficiency. The proposed key establishment scheme can be used not only for establishing shared key between any two sensors, but it is applicable for establishing shared secret between any two entities/ things in the context of IoT.

Keywords

Internet of Things (IoT), Wireless sensor network (WSN), Key establishment , Internet Protocol for Smart Objects.

1. INTRODUCTION

In the upcoming Internet of Things (IoT), the everyday objects that surround us will become proactive actors of the Internet, generating and consuming information. The elements of the IoT comprise not only those devices that are already deeply rooted in the technological world (such as cars or fridges) [1], but also objects foreign to this environment (garments or perishable food), or even living beings (plantations, woods or livestock). By embedding computational capabilities in all kinds of objects and living beings, it will be possible to provide a qualitative and quantitative leap in several sectors: healthcare, logistics, domotics, entertainment, and so on.

In fact, one of the most important elements in the IoT paradigm is wireless sensor networks (WSN). The benefits of connecting both WSN and other IoT elements go beyond remote access, as heterogeneous information systems can be able to collaborate and provide common services. Internet-enabled WSNs can be used to bridge the physical world that we inhabit with the virtual world of the Internet [2]. Miniature battery-operated sensors with wireless connectivity and processing capability which are attached to objects can be used to extend the connectivity of the Internet. Information from the sensory data can be used to build web-oriented applications such as smart metering and smart building networks, and a number of bodies have been active in their standardization.

The Internet Protocol for Smart Objects (IPSO) Alliance [3] has been involved in the interfacing of IP technology with everyday physical devices. In addition, the Internet Engineering Task Force (IETF) has incorporated several Working Groups towards the standardization of IP protocols for these objects. Their first attempt was to compress IPv6 over Low power Wireless Personal Area Networks (6LoWPAN) [4] to enable its use in low-power 802.15.4 radios. The Routing Over Low power and Lossy networks (ROLL) Working Group is promoting a routing protocol called the IPv6 Routing Protocol for Low-power and Lossy networks (RPL) [5].

Many applications of sensor networks require secure communication. Thus establishing a secure channel between any two sensor-nodes in WSNs/IESNs is important for many applications, such as secure data exchange, secure data aggregation, and secure routing.

Internet-enabled WSNs can be realised by adapting traditional web protocols in ways suitable to different applications, thereby enabling the integration of these sensor-enriched physical objects to the Internet. This can be made possible if the existing REpresentational State Transfer (REST) architectural style can be extended to accommodate new application layer protocols suitable for WSNs over existing transport protocols such as TCP/ UDP.

The IETF Constrained RESTful Environments (CoRE) Working Group [6] is focusing on designing application layer protocols that manipulate sensor data, which overcome the restrictions of their networking environments. The resulting Constrained Application Protocol (CoAP) [7] integrates the different facets of the web service architecture. CoAP includes a subset of the REST features that are available in HTTP, to enable effective Machine-to-Machine (M2M) communication between devices.

There are some security challenges in IESN or internet enabled wireless sensor network. They are node mobility, authentication process between nodes, resilience, Bit/signal transmission distance, Key connectivity, energy efficiency, bandwidth and Scalability. To overcome these security challenges proposing a new key establishment scheme in order to obtain the secure communication in internet enables wireless sensor network. In addition to these the proposed methodology detects the attacks such as Sybil and Dos attack for identifying the compromised node.

2. RELATED WORK

Ibriq & Mahgoub (2014) [8] presented a hierarchical key establishment scheme called HIKES. The base station in this scheme, acting as the central trust authority, empowers randomly selected sensors to act as local trust authorities authenticating, on its behalf, the cluster members and issuing private keys. HIKES uses a partial key escrow scheme that enables any sensor node selected as a cluster head to generate all the cryptographic keys needed to authenticate other sensors within its cluster. This scheme localizes secret key issuance and reduces the communication cost with the base station. HIKES provide an efficient broadcast authentication in which source authentication is achieved in a single transmission and a good defense for the routing mechanism. A HIKE defends the routing mechanism against most known attacks and is robust against node compromise. A HIKE also provides high addressing flexibility and network connectivity to all sensors in the network, allowing sensor addition and deletion.

Newell et al (2014) [9] identify the main factors influencing the design space of key management protocols for sensor networks and describe representative protocols that trade off the number of links established, communication overhead, and resilience to node capture. This trade-offs are due to using direct, pathbased, or multipath-based communication to establish secure links. The author propose a new multipath protocol relying on an encoding scheme tailored for WSNs and analyze the effects of key pre-distribution on multipath key establishment. The author provide extensive simulations to understand the trade-offs between resilience to node compromise and communication overhead under numerous network scenarios. This comparison highlights the trade-offs between these vastly different key management schemes.

SNEP [10] and BBF [11] are two well-known schemes in Arbitrated keying category, which are illustrated in Fig. 1. The node A, as a new node, wants to establish a shared secret with the node B. There is a server, S, which is a trusted third party to establish shared secrets between nodes. As will be elaborated in the next section, both of these methods have a kind of DoS vulnerability, which lead to a significant waste of power and lifetime in nodes. The steps of protocols and exchanged messages are mentioned in the figure.

Lasla proposed a novel secure routing protocol named Secure Multi-pAths Routing for wireless sensor neTworks (SMART) as well as its underlying key management scheme named Extended Two-hop Keys Establishment (ETKE) [12]. The proposed framework keeps consistent routing topology by protecting the hop count information from being forged. It also ensures a fast detection of inconsistent routing information without referring to the sink node. We analyze the security of the proposed scheme as well as its resilience probability against the forged hop count attack. We have demonstrated through simulations that SMART outperforms a comparative solution in literature, i.e., SeRINS, in terms of energy consumption.

Khan et al (2014) [13] proposed a new authentication and key management scheme for heterogeneous sensor networks including mobile nodes. The relevant network and mobility models have been presented as well. The proposed key management scheme is based on two different types of the key pools, that is, an authentication key pool and a communication key pool. Based on these pools, a key pre-distribution mechanism has been defined. Moreover, we compared our solution with some of the existing key management protocols for both homogeneous and heterogeneous sensor networks.

Roy & Das [14] proposed scheme adopts a level based secure hierarchical approach to maintain the energy efficiency. It incorporates light-weight security mechanisms like, nested hash based message authentication codes (HMAC), Elliptic-Curve Diffie-Hellman (ECDH) key exchange scheme and Blowfish symmetric cipher. Simulation results show that the scheme performs better than existing secure routing protocols FBSR and ATSR.

MiniSec [15] is a secure network layer that obtains the best of both worlds: low energy consumption and high security. MiniSec has two operating modes, one tailored for single-source communication, and another tailored for multi-source broadcast communication. The latter does not require per-sender state for replay protection and thus scales to large networks. We present a publicly available implementation of MiniSec for the Telos platform, and experimental results demonstrate our low energy utilization.

Ge & Choo (2014) [16] propose a novel key revocation scheme which is a hybrid of centralized and distributed methods. The design of our scheme is based on Chan et al. [17] but eliminates the requirement of prior knowledge. It mainly consists of a voting procedure among nodes and a global revocation by the base station. The author also modify existing distributed revocation properties in Chan et al. [17] protocol and extend them to key revocation properties of any hybrid schemes based on the voting process.

Liu & Zhao (2015) [18] adopt the bilinear pairing theory to the public key generation and management which does not require the public key in the nodes and applies the node's information to the public keys, which may reduce the cost of managing the public keys and enhances the security of key management; then we propose a cluster key distributed scheme on the basis of clustering by using the bilinear pairing key management in the wireless sensor network and demonstrate its feasibility and security theoretically.

3. PROPOSED METHODOLOGY

In this section, we introduce our extension to fix the problem.

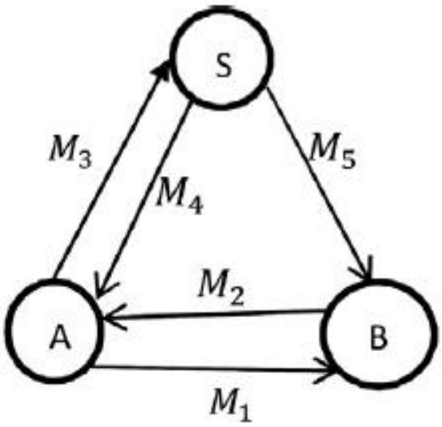
We consider five types of Messages, as shown in Fig. 1. Type 1, M1, is used as a request message and is locally broadcast by a new node. Type 2, M2, is built and locally broadcast by the interested neighbors as response after receiving M1. Type 3, M3, is built by the new node after receiving all messages of type M2. The type 4 and 5, (M4 and M5), are built by the server S and include secret key for the new node and neighbors, respectively. Assume that the node A in Fig. 1 wants to join the network by establishing shared secrets with its d neighbors including the node B. The process is done as follows:

Key establishment request: As soon as ending the network initialization time, sensor nodes will start secure communication among themselves. When a new node, A, wants to join the network after initialization time, it is required to work based on a challenge/response scheme. At the first step a request message, M1, is locally broadcast to interested neighbors. Following is the format of M1 where | specifies concatenation:

$$M_1 = ID_A | N1_A$$

The nonce N1A inhibits the replay attack, which will be discussed later.

Response message: All the sensor nodes in the transmission range of the node A that receive M1, (e.g. the node B), will locally respond by broadcasting M2, if they are interested to establish a secret key with A. The format of M2 is as follows:



$$M_1 = ID_A|N1_A \quad M_2 = ID_A|ID_B|N1_A|N_B$$

$$M_3 = ID_A|N2_A|NeiSet_A|MAC(K_{SA}^{'}, ID_A|N2_A|NeiSet_A)$$

$$M_4 = \{K_{AB}\}_{SA} MAC(K_{SA}^{'}, K_{AB}|ID_B|N2_A)$$

$$M_5 = \{K_{AB}\}_{K_{SB}} |MAC(K_{SB}^{'}, K_{AB}|ID_A|N_B)$$

Fig. 1. Message flow in the proposed extension. The hash key inferred from the encryption key, as K0 = g(K).

This message consists of the identifier and the nonce of both nodes, A and B.

Construction of message type 3: The new node A, after receiving all messages of type M2, constructs a message M3 which is concatenation of A's identifier, A's second nonce (N2A) and the set NeiSetA. The set NeiSetA is a set of pairs of identifiers and nonces of the interested neighbors of A. The identifiers in NeiSetA show the neighbors of A that are interested to establish a pair-wise key with A. The nonce N2A is used to check strong freshness and will be discussed later.

$$M_3 = ID_A|N2_A|NeiSet_A|MAC(K_{SA}^{'}, ID_A|N2_A|NeiSet_A)$$

$$NeiSet_A = ID_X|N_X| \ldots.$$

At the network initialization time, any node, like A, contains a master individual key, KSA, which is the master key between A and the server, S. We generate MAC (Message Authentication Code) as K0 = g(K). We do not use one key in two succeeding operations, to achieve more security [9].

Operations in the server S: The shared secret key is made in the server S and would be securely transferred to sensor nodes. Node S after receiving M3, checks replay attack on M3 by N2A. After this stage, S constructs a pair-wise key, KAB, between A and B. This would be done by a pseudo random function f, which has enough security. Function f acts as follows:

$$K_{AB} = f(ID_A|ID_B|N2_A)$$

After generating K_{AB} messages $M_4 and\ M_5$ would be constructed as follows

$$M_4 = \{K_{AB}\}_{SA} MAC(K_{SA}^{'}, K_{AB}|ID_B|N2_A)$$

$$M_5 = \{K_{AB}\}_{K_{SB}} |MAC(K_{SB}^{'}, K_{AB}|ID_A|N_B)$$

The message M4 consists of the encrypted secret key KAB and a MAC value. The MAC value is digestion of concatenation of the secret key, the identifier of the node B and the second nonce N2A. The encryption is done by the individual master key KSA shared between S and A. The message M5 is similar to M4 and consists of the encryption of the generated secret key and a MAC value. The MAC value is digestion of concatenation of the secret key, the identifier of the node A and the nonce NB. Other IESN and IoT nodes are unaware about KAB, because they do not have KSA and KSB. In fact, the server S, generates messages of type 5 as many as the number of interested nodes (here, for simplicity, we have only mentioned the node B).

4. EXPERIMENTAL RESULTS

The performance evaluated based on the parameters computational cost , Communication cost, Total Energy Cost, Security and DOS.

Computational Cost

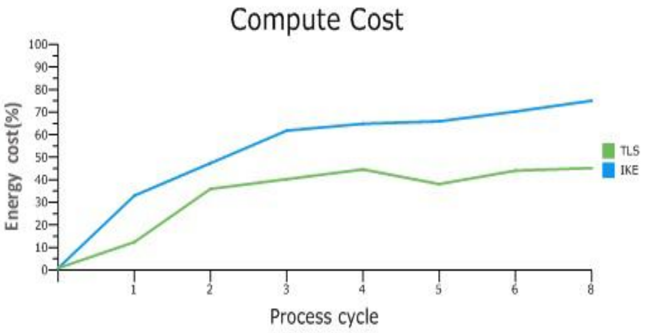


Figure 2 Comparison based on Computational Cost

Figure 2 illustrates the comparison of test programs for individual computational operations were run on an Intel i3 processor and the corresponding number of processor cycles for each was retrieved. In order to be able to induce the number of cycles measured on a resource constrained device from the number of cycles on a powerful processor, it disabled advanced features of our test processor (hyperthreading, multicore, variable clock speed).

Communication Cost

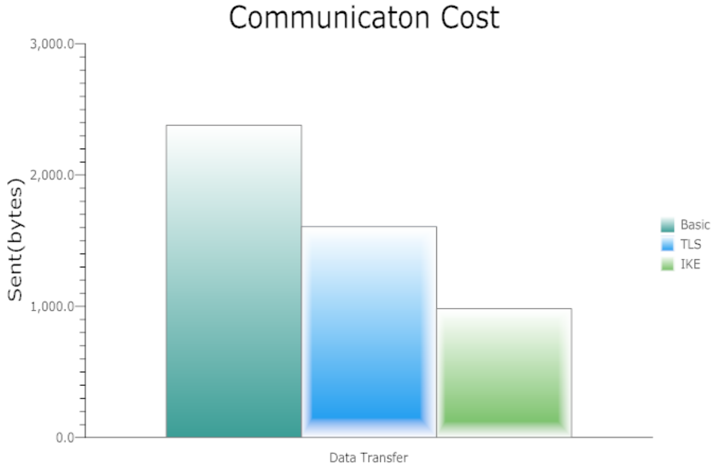


Figure 3 Comparison based on Communication Cost

Figure 3 illustrates the comparison number of exchanged bytes by the source node in TLS Handshake [4] and IKE protocols considering both the basic exchange and the distributed approaches. Consider that the constrained node is listening during a delay corresponding to the latency of communications (Tx, Rx) and packets propagation (D) as well as the processing of packets at the proxies and the responder. Estimate below the listening durations required by the constrained node.

Assuming that the server is an unconstrained node while proxies are 10 times less constrained than the server, this duration is respectively 401 ms and 404 ms for TLS Handshake and IKE while it respectively amounts to 411 ms and 446 ms for the distributed TLS Handshake IKE approaches.

Total Energy Cost

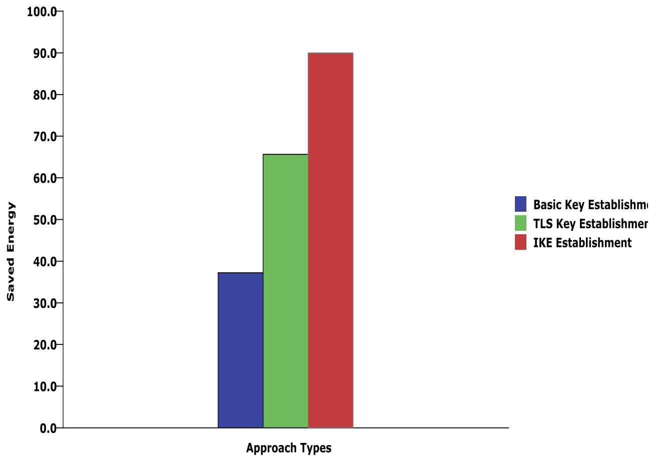


Figure 4 Comparison based on Total Energy Cost

Figure 4 illustrates the comparison the computed costs confirm the efficiency of the cooperative scheme proposes. The most significant energy savings concern the key agreement mode . They amount to 90% of what is consumed in IKE protocol. Concerning the key transport of TLS handshake, the constrained node saves around 35% of its energy, as compared with what is spent during the basic exchange.

These results were expected since delegating the computation of DH modular exponentiations (in the key agreement mode) leads to more energy savings at the constrained device than offloading signature and encryption operations in the key transport mode. Energy savings can be increased by reducing the duration of listening mode.

Security

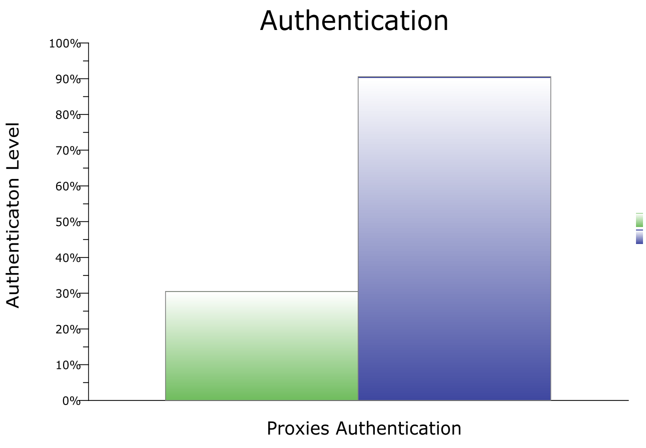


Figure 5 Comparison based on Security

Figure 5 illustrates the comparison first point of focus of the present security analysis consists in dealing with malicious proxies in order to ensure a fair level of security even in case of their presence. The selection of multiple proxy nodes at the constrained device represents the main protection against key compromising, since a single proxy will only get access to a part of the secret the more numerous the proxies, the smaller the fragment disclosed to each proxy. Selecting the right number of proxies should be a function of the network size and topology, the degree of resilience required against attacks and the quantity of resources that a proxy is devoting to collaborative services. It is evident that choosing a small number of proxies causes a bottleneck and creates performance problems while selecting a high number of proxies increases the communication and, in certain cases, computational overhead during the protocol exchange.

DOS

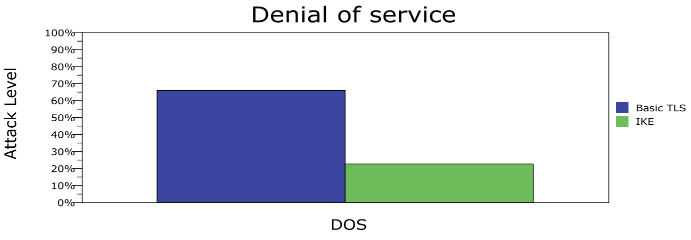


Fig 6 Comparison based on Dos

Figure 6 illustrates the comparison Denial of Service (DoS) attacks against our solution would consist in unfair playing or malicious proxy trying to disrupt the collaborative key establishment protocol by sending no or bogus traffic to the server. Without an adapted protection scheme, a selfish proxy could paralyze the whole system and make the key establishment between the constrained source node and the server fail. This kind of ‘‘unfair’’ play has been carefully considered in the design of our solution. Preventing this type of misbehaviour is obviously the keystone of protection against malicious nodes.

This latter detects the non-cooperative proxies when reassembling the premaster secret or recovering the DH public key and reports a feedback to the constrained source node containing the list of participating proxies. Thereby, the constrained node learns the identities of misbehaving proxies and will prevent their selection in the future.

5. CONCLUSION

It is clear that the potential of the wireless sensor networks (WSN) paradigm will be fully unleashed once it is connected to the Internet, becoming part of the Internet of Things (IoT). In this paper, a new three party key establishment scheme for Internet-enabled sensor networks as part of Internet-of-Things was proposed. We introduced our key establishment scheme based on traditional Internet style key establishment and long-term master-individual keys as a DoS resistant version of two well-known previous schemes. In comparison to the previous well-known three-party schemes, our extension not only fixes DoS vulnerability, but also provides some other advantages such as significant efficiency. The proposed key establishment scheme can be used not only for establishing shared key between any two sensors, but it is applicable for establishing shared secret between any two entities/ things in the context of IoT.

6. ACKNOWLEEDGEMENT

First and foremost I place this project work on the feet of GOD ALMIGHTY who is the power of strength in each step of progress towards the successful completion of my project. I am highly indebted to Dr.N.R.Alamelu, M.E., Ph.D. Principal, Sri Ramakrishna Engineering College, Coimbatore for providing the required facilities and support to carry out this project work. I extend my heartfelt thanks to Dr.A.Grace Selvarani, M.E., Ph.D. Professor and Head, Department of Computer Science and Engineering (PG), who had been a source of inspiration and for her timely guidance in the conduct of this project work. I am grateful to Dr.J.Selvakumar, assistant professor, Department of Software Engineering(PG), for his able guidance and useful suggestions which helped me in completing the project work in time. Finally, I would like to express my heartfelt thanks to my beloved parents for their blessings, my friends for their help and wishes for the successful completion of this project.

7. REFERENCE

[1] Radoi, I. E., Shenoy, A., & Arvind, D. K. (2012, June). Evaluation of routing protocols for internet-enabled wireless sensor networks. In *ICWMC 2012, The Eighth International Conference on Wireless and Mobile Communications* (pp. 56-61).

[2] G. Montenegro, N. Kushalnagar, J. Hui, D. Culler. RFC 4944: Transmission of IPv6 Packets over IEEE 802.15.4 Networks. 2007.

[3] IPSO Alliance, http://www.ipso-alliance.org/, [April 2012].

[4] T. Yang, M. Ikeda, G. DeMarco, and L. Barolli, “Performance Behavior of AODV, DSR and DSDV Protocols for Different Radio Models in Ad-Hoc Sensor Networks”, in Proc. Int. Conf on Parallel Processing Workshops, Sept. 2007.

[5] K.J. Wong and D.K. Arvind, “SpeckMAC: low-power decentralised MAC protocols for low data rate transmissions in specknets.” Proceedings of the 2nd international workshop on Multihop ad hoc networks from theory to reality. ACM, 2006. 71-78.

[6] P. Levis, N. Lee, M. Welsh, and D. Culler, “TOSSIM: Accurate and scalable simulation of entire TinyOS applications,", 1st Int. Conf. On Embedded Networked Sensor Systems. ACM, 2003, pp. 126 – 137.

[7] Z. Shelby, K. Hartke, and B. Frank, “Constrained Application Protocol (CoAP) draft-ietf-core-coap-08”, Nov. 1, 2011.

[8] Ibriq, J., & Mahgoub, I. (2014). HIKES: Hierarchical key establishment scheme for wireless sensor networks. International Journal of Communication Systems,27(10), 1825-1856.

[9] Newell, A., Yao, H., Ryker, A., Ho, T., & Nita-Rotaru, C. (2014). Node-Capture Resilient Key Establishment in Sensor Networks: Design Space and New Protocols. ACM Computing Surveys (CSUR), 47(2), 24.

[10] Perrig A, Szewczyk R, Tygar JD, Wen V, Culler DE. Spins: security protocols for sensor networks. Wirel Netw 2002;8(5):521–34.

[11] Bauer RK, Berson TA, Feiertag RJ. A key distribution scheme using event markets. ACM Trans Comput Syst 1983;1(3):249–55.

[12] Lasla, N., Derhab, A., Ouadjaout, A., Bagaa, M., & Challal, Y. (2014). SMART: Secure Multi-pAths Routing for wireless sensor neTworks. In Ad-hoc, Mobile, and Wireless Networks (pp. 332-345). Springer International Publishing.

[13] Khan, S. U., Lavagno, L., Pastrone, C., & Spirito, M. A. (2014). Online Authentication and Key Establishment Scheme for Heterogeneous Sensor Networks. International Journal of Distributed Sensor Networks, 2014.

[14] Roy, S., & Das, A. K. (2014). Secure Hierarchical Routing Protocol (SHRP) for Wireless Sensor Network. In Security in Computing and Communications (pp. 20-29). Springer Berlin Heidelberg.

[15] Luk, M., Mezzour, G., Perrig, A., & Gligor, V. (2007, April). MiniSec: a secure sensor network communication architecture. In Proceedings of the 6th international conference on Information processing in sensor networks (pp. 479-488). ACM.

[16] Ge, M., & Choo, K. K. R. (2014). A Novel Hybrid Key Revocation Scheme for Wireless Sensor Networks (pp. 462-475). Springer International Publishing.

[17] Chan, H., Gligor, V.D., Perrig, A., Muralidharan, G.: On the Distribution and Revocation of Cryptographic Keys in Sensor Networks. IEEE Transactions on Dependable and Secure Computing 2(3), 233–247 (2005)

[18] Liu, X., & Zhao, Q. (2015, January). Cluster Key Scheme Based on Bilinear Pairing for Wireless Sensor Networks. In Proceedings of the 4th International Conference on Computer Engineering and Networks (pp. 299-304). Springer International Publishing.