Analysis and Comparison of Key Revocation Protocols in Wireless Sensor Network

[1]Taofeek, Yusuf
Cyber Security Science Department
Federal University of Technology
Minna, Nigeria
taofeekyusuf.920@gmail.com

[2] Victor, Onomza Waziri
Cyber Security Science Department
Federal University of Technology
Minna, Nigeria
victor.waziri@futminna.edu.ng

[3] Bashir, Mohammed Abdullahi
Computer Science Department
Federal University of Technology
Minna, Nigeria
el.bashir02@futminna.edu.ng

[4] ,Morufu Olalere
Cyber Security Science Department
Federal University of Technology
Minna, Nigeria
lerejide@futminna.edu.ng

Abstract—The need for efficient and secure key revocation protocols in Wireless Sensor Networks (WSNs) is a challenge in the design of protocols that will meet the severe constraints that characterized the WSNs. This study presents analysis and comparison of centralized key revocation protocols in WSNs. In this context, the study presents the representative number of centralized key revocation protocols and a comparative summary of their significant features. The authors carried out a security and performance analysis of the presented protocols based on security goals of confidentiality, integrity, authenticity, availability and their related attacks. Finally, the work compares their security and performance metrics, with the aim of identifying efficient and secure key revocation alternatives.

Keywords— Wireless Sensor Network, Key Management, Key Revocation, Intrusion Detection System

I. INTRODUCTION

Wireless Sensor Network provides cost effective solutions to many real life challenges, which makes them useful in many applications. WSN is applied in application areas such as healthcare systems for monitoring of patient's conditions, environmental tracking, transportation systems, and military operation [1]. Security is a challenge and an issue of grave concern in WSN, because sensor nodes in the network transmit sensitive information. WSNs are vulnerable to diverse attack types due to their constrain computational resources and fully distributed nature. The moment a secure communication is established in the network. Situation might arise, such that, a node in the network can run out of battery. Additional node can join the network, possibilities are also that an intruder could capture a node and collect the secret data. An attacker could join the network and be part of the nodes in the network [2]. Once a node is discovered to be a victim of the various compromised mentioned, the next stride is to invalidate the malicious nodes identified and then replaced the cryptographic keys used in the affected network [3].

Relative to WSNs, key management protocols are made up of the following process, key generation, key agreement, key distribution, and key revocation (KR), the former methods have been more extensively study, even though key revocation has been receiving relatively low attention [4]. This work aims to compare and identify the most appropriate protocol for future research and their suitability to meet the security and performance requirements in their applications. The following KR protocols are to be considered: Key Management and Distribution Framework (KMMR)**,** Secure Key Revocation and Renewal Protocol (SKRR)**,** Key Updating for Removing and Replacement of Compromised Sensor Nodes (KURCS) In a WSN**,** Key Revocation Scheme for WSNs (KeyRev)**.**

The research contribution is the analysis of the four KR protocol considered. The security and performance of the four protocols were compared base on some standard metrics in the literature. These analyses will provide WSN implementation and the research community with efficient and secure key management protocol options. The rest of the paper is organized as follows. Section II present related work and the summary of the notations used throughout the work, section III covers the presentation of the categories key revocation protocols in the study. In section IV, the security and performance analysis of the considered protocols are carried out, this is followed by a comparative summary of their security and performance metrics. Finally, section V discussed the conclusion and future direction of the work.

II. RELATED WORK

Several techniques are proposed in order to address the challenges associated with key revocation in WSNs in the literature. The proposed techniques include centralized, distributed, and hybrid schemes. Prominent among the pioneering work on key revocation protocols is the work of [5], the authors proposed a scheme that is designed to fulfill the distributed sensor network operation and security requirements. The scheme is simple to implement, scalable and flexible; however, the scheme is vulnerable to revocation attack, since an adversary can use the key distribution mechanism in the revocation protocol to revoke uncompromised nodes in the network, in addition, to distribute a signature key in a network of size n it requires n unicast message exchange. In order, to address some of the weaknesses in [5], several modified approaches have been presented. The authors in [6] proposed a key revocation protocol that is scalable and guarantee an authenticated distribution of keys with efficient storage, computing and communication overheads, the protocol uses a key service, which is capable of revoking existing set of keys and redistributes new keys to all nodes except for the compromised one. Nevertheless, the use of a one-way function can cause the scheme to witness delay authentication of messages, which will negatively impact on the energy overhead of the protocol.

The authors in [7] proposed a centralized key revocation scheme that aimed at addressing some of the observed deficiencies in the previous works, the scheme obsolete keys owned by the compromised node from the network, through key updating techniques that discard the compromised node from the network. However, the session key update timing is a challenge, since a delay in the session key update could lead to the disclosure of the encryption and MAC keys which the adversary can use to carry out injection attacks or further compromise other nodes. [8] proposed another key revocation protocol named mKeyRev, to address some observed challenge with KeyRev. The proposed study includes a key distribution scheme that supports multiple base station and a key revocation scheme designed to discard compromised sensor nodes from the WSNs efficiently. However, the scheme cannot defend against Denial of service attacks (DoS) and no clear means of dealing with compromised nodes before the next session key update. [9] proposed a hybrid of centralized and distributed approach, and the scheme uses autonomous generation and distribution of secret shares by sensor nodes to exclude prior knowledge constraint with the use of the base station to achieve a total revocation in the network. The scheme addresses the issue of a single point of failure associated with centralized key revocation schemes. However, the scheme leads to a more complex network design. The authors in [3], propose a secure protocol for key revocation and renewal which is based on symmetric and asymmetric cryptographic primitives, the revocation process involves the collection of IDS result by the sink which serves as the bases for determining the nodes that will be revoked, then a revocation message is sent to initiator node with the list of the compromised nodes in the neighborhood of the initiator node, the authentication of communication is guaranteed in the protocol. Nevertheless, the successful execution of the KR depends on the accuracy of the IDS result and the revocation decision solely taken by the sink.. [10] present a node revocation protocol for secure multi-hop communication in large scale WSNs, in their work, the detection of the compromised node is through an intrusion detection systems (IDS) which generate secure report messages that contain local occurrences and acquired neighbor's monitored information, which is sent to the base station from the sensor nodes. The protocol gives the desired resilience to wide WSN and damages is restricted to the direct links with compromise nodes, however, the protocol does not state the type of symmetric cryptographic primitives employed.

TABLE I. THE LISTED ITEMS SUMMARIZE THE NOTATIONS USED THROUGHOUT THIS WORK

Notation	Description
SRM	Denotes Secure Report Message
BS	Base Station
MAC	Message Authentication Code
PWK	Denotes Pairwise Key
LBK	Local Broadcast Key
GBK	Global Broadcast Key
SAKUM	Secure Acknowledgement key update message
S	Base Station of the Network
Enc_{INK}	Encryption of Individual Key
n_s	Nonce Generated by The Sink
NK'	New Network Key

III. CATEGORIES OF KEY REVOCATION PROTOCOLS IN WSN

This work presents categories of existing key revocation protocols based on the work of [4]. The protocols are classified into four broad categories: Centralized, Distributed, Decentralized, and Hybrid. In WSNs, designating a protocol to a class depends on the level of its involvement with a central authority, hence, to provide a thorough analysis and comparison of the KR protocols, this work will focus on centralized KR with respect to their performance and security as shown in figure I. Reference [4] provide information on categories of the KR protocols in details.

A. centralize key revocation protocols in WSNs

Key revocation is a process that involve secure withdrawal or invalidation of the key information that relates to any malicious or compromised node in the networks. In the centralized key revocation protocols, the revocation decisions are usually taken by a single appointed authority [11]. The four considered key revocation protocols play significant role in various revocation application. They also provide accurate evidences of desired properties in their implementations. The criteria for their selection are, resilient to revocation attacks, unitary revocation and regulated time revocation completion. The selected protocols represent the various class of centralized key revocation protocols which are presented in the following sections.

The centralized key revocation protocol was first presented in [5]. In the centralized key Revocation protocols, the revocation decisions are usually taken by a single appointed authority. In situations, where misbehaving sensor nodes are noticed in the network, it is required that the central authority revoke the compromised nodes by removing compromise keys or updates keys. The basic difference between decentralize and distributed KR is that, in distributed KR, the process of node revocation requires collaboration among nodes in the network, while in distributed KR the decision to remove a compromised node is made by a single node [4]. The revocation process does not involve a central authority and the cooperation of other nodes, hence the scheme provide a fast means of revoking compromised nodes.

In hybrid revocation scheme, the revocation protocol depends on the concept of grouping nodes, the process involves the combination of both distributed and centralized methods in order to increase revocation efficiency and accuracy.

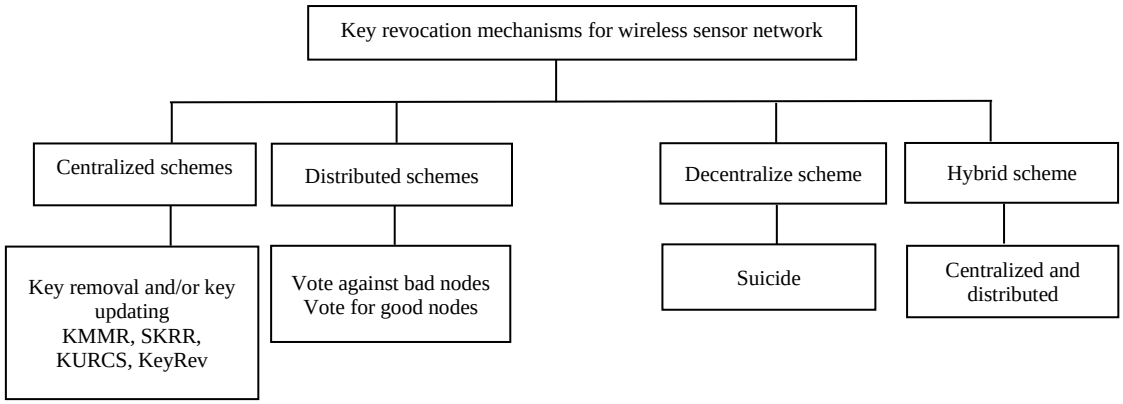

Fig. 1. Taxonomy of key revocation protocols in WSNs

B. Key Management and Distribution Framework (KMMR)

The authors in [10] proposed a protocol that prioritizes the operation of IDS in the base station to provide secure communication in a sensor network. The collection of local events and neighbors tracking information contained in the Secure Report Message (SRM) are sent to the base station by the sensor nodes.

$$SRM\ (S \rightarrow BS):$$

$$Router\ ID\ Time\ stamp, Enc_{INK}, MAC_{PWK}\ (M)$$

Upon detection of compromised nodes by the IDS, the BS broadcasts an Authenticated Broadcast of Alarm Message (ABAM) that includes a blacklist. The authentication of ABAM is through the delayed disclosure of the hash key K_{j+1}.

$ABAM(BS \Rightarrow^{*})$:

$K_j, Enc_{GBK}(Backlist), MAC_{Kj+1}\ MAC_{LBK}\ (M)$

The BS sends the Hash key Disclosure of Alarm Message (HKDAM), the sensor node S is capable of verifying the authenticity of the BAM, when the hash key K_{j+1} is revealed. Firstly, the shared PWK that is carried by the malicious nodes is erased by the healthy nodes and then generate the new LBK. A Secure key Update Message (SKUM) protected with the PWK is sent to the healthy neighbor S' in order to share the LBK.

$SKUM(S \rightarrow S')$:

$NonseS, Enc_{PWK}(LBK), MAC_{PWK}(M)$

A Secure Acknowledgement of key Update Message (SAKUM) from individual healthy neighbor S' received by node S confirms the sharing of the new LBK. Consequently, it will be impossible for the compromised node to interpret secure local broadcast messages.

$SAKUM(S' \rightarrow S)$: $NonceS', Nonce, MAC_{PWK}\ (M)$

And finally, the GBK is updated by the BS.

C. Secure Key Revocation and Renewal Protocol (SKRR)

SKRRP was presented by [2], they proposed a secure key renewal and revocation protocol for WSN which is based on AES and ECC cryptographic primitives. Before there deployment, the sensor nodes are preloaded with public key of the sink $pk(S)$ and their public and private key pair, denoted as $pk(N)$ and $sk(N)$ respectively. In the revocation process, the result received from the IDS is used as the bases for identifying compromised node by the sink. In the event that a sink detects a malicious neighbor of node N, a revocation message is sent to node N. The message sent contains a list of compromised nodes and a nonce ns encrypted with $K_{DH}\ (S, N)$.

As soon as N received the message, it deletes the season keys shared with all the neighbor nodes that appear on the list and sends back ns encrypted with $K_{DH}(N, S)$, in order to affirm the receipt of the revocation message. There is also the need for the sink to renew the network key, when nodes in the network have been compromised. Therefore, the sink computes a new network key NK' and a nonce $n_{(si)}$ for every healthy node using $K_{DH}\ (S, I)$ and send the encrypted message to I. Upon receiving the message, I send back the encrypted $n_{(si)}$ using $K_{DH}\ (S, I)$, the sink then wait until it received all nonce before the use of the NK' can commence.

D. Key Updating for Removing and Replacement of Compromised Sensor Nodes (KURCS) In a WSN.

The authors [12] presents a general framework, to efficiently remove and replace compromised sensor nodes in a WSNs, based on the work of [13] compromised nodes detection scheme. The scheme split the network into a static cluster, where cluster members are fixed and made permanent for the period of the network existence, each cluster is provided with one cluster guard in order to balance the energy need amid all cluster members, one cluster head is chosen among all cluster members in each round on rotational basis. A secret key is shared between each sensor node in the network, and the base station usually refers to as the base station key. Once a node is identified as being compromised, the cluster guard immediately generates a new cluster key generation parameter (seed value), which is unicasted to every cluster member with the exception of the compromised nodes using the shared cluster guard key of

the cluster guard and the individual cluster members. Key updating: the concept of one key one time (OKOT) is adopted on cluster and sensor keys. A key is updated anytime the key is used, and for each round of communication, the cluster key is used since different cluster head is elected by all the cluster members on a rotational basis of each round in order to balance the energy used.

E. Key Revocation Scheme for WSNs (KeyRev)

In KeyRev presented by [7], to achieve secure communication, each sensor node in the network maintains a node revocation list (NRL). A node revocation list contains all the sensor identifiers that have been revoked in the WSN. The population in the revocation list is usually empty at the onset of the network, but increases as time progresses. For secure information exchange in sensor network, two different keys are proposed by the authors, they include the encryption key K_{encr} and the Message Authentication Code (MAC) Key K_{mac}. At every update of the session key K_j, both keys will change simultaneously. In order to achieve all this, the authors introduced the session key sharing scheme proposed by [14].

In the broadcast phase of the scheme, the base station broadcast to the non-compromised nodes in the network a message in this format: $B = R \cup \{P_j(x)\} \cup \{Q_J(x)\}$ Where $P_j(x)\ and\ Q_J(x)$ are acquired using a fixed revoked group numbers in the session j or the received list R.

$R = \{r_1, r_2, \dots, r_3\}$, with $w \leq t$ and a t-degree polynomial $P_j(x)$ that is picked in the setup phase randomly by the setup server.

In order to get back the session key by any non-compromised node i that received such a broadcast message, node I will compute the polynomials.

$P_j(x)$ and $Q_j(x)$ at point j so as to get the new session key. Hence, the possibility of stopping the compromised node from deriving the K_{encr} and K_{mac} by preventing them from acquiring the current session key. Therefore, the compromised node is securely eliminated from the sensor networks

TABLE II. COMPARISON OF MAJOR FEATURES OF THE CENTRALIZED KEY REVOCATION PROTOCOLS

Protocol	Standard Algorithm	Cryptographic Techniques	Detection Techniques	Revocation Techniques	Evaluation Techniques
KMMR	Yes	AES	IDS	Erase PWK	Implementation
SKRR	Yes	AES and ECC	IDS	Delete session key	Implementation
KURCS	No	Virtual location key generator	Trust establishment model	Key updating	Simulation
KeyRev	No	Pseudo-Random function	N/A	Key updating	Simulation

IV. SECURITY AND PERFORMANCE ANALYSIS OF THE CENTRALIZED KEY REVOCATION PROTOCOLS IN WIRELESS SENSOR NETWORKS

This part of the work shall discuss and analyses the security of each of the considered solutions as well as their performance in terms of computation, communication, energy and storage cost.

A. Security Analysis

The analysis of these protocols shall be based on the fundamental security goals of confidentiality, integrity, availability, authenticity, and freshness with respect to their associated attacks scenario. The assumption in most centralized KR protocol is that an intrusion detection system (IDS) is deployed to initiate the discovery of compromised nodes before their revocation from the network, to perform the revocation task, central authority, also called the base station (BS) is required to communicate with sensor nodes securely and be responsible for conducting the revocation decisions. One major setback with this type of scheme is the single point of failure. An attacker may impersonate the central authority and start launching revocation attacks.

In order to be resilient to revocation attacks, KMMR, SKRR, and KeyRev used the authentication broadcast messaging, which makes it impossible for the adversary to prevent the broadcast message from reaching the designated sensor nodes, thus the trio of KMMR, SKRR and KeyRev are resilient against revocation attacks. In addition, the use of nonce prevents the replay of old messages in KMMR and SKRR, hence their ability to guarantee data freshness and resilient against replay attacks. Furthermore, the implementation of secure node addition by KeyRev, KMMR, and SKRR protocols ensures protection against black-hole and Sybil attacks. Both SKRR and KeyRev are resilient to node capture attacks, and this is due to their prompt update of the session key. Similar to KeyRev, the use of OKOT principle by KURCS, enable the protocol to protect against node compromise and replication attacks.

Finally, to guarantee an end to end secrecy of data exchange in a protocol, the use of public-key cryptography is crucial, in this context, only SKRR scheme combines the capabilities of the symmetric and public key cryptographic algorithm in their implementation.

TABLE III. COMPARISON OF SECURITY FEATURES OF THE CENTRALIZED KEY REVOCATION PROTOCOLS

Protocols	Forward and Backward Secrecy	Revocation Attacks	Sybil Attacks	Node Capture Attacks	Replay Attacks
KMMR	Forward	Yes	Yes	Yes	Yes
SKRR	Both	Yes	Yes	Yes	Yes
KURCS	Forward	No	No	Yes	Yes
KeyRev	Forward	Yes	Yes	Yes	No

B. Performance analysis

In order to measure the performance of the four KR protocols considered, the study examine their evaluation techniques as shown in Table II. Then analyze each protocol based on the evaluation experiments and then compare the performance of each protocols.

Energy consumption: In KURCS, the use of cluster reduced the energy consumption of the network through reduced long-distance transmission of the participating nodes. The SKRR protocol implementation is based on symmetric encryption and elliptic curve cryptographic primitives, the mentioned algorithms are very strong and required higher energy consumption when compared to KMMR that was implemented base on AES algorithm.

In KeyRev, the average energy consume to invalidate a node that is compromised in the network involves a broadcast message to all non-revoked sensor nodes and the appraisal of the polynomial $P_j\ (x)\ and\ Q_J(x)$ at a point i. In KMMR, the design aims at accomplishing energy efficiency, and the solution implements the tier-based architecture, where the process of establishing all it shared key is organized into upward and downward phases, this is done to reduce the number of data transmission which will in turn impact on the energy consumption of the network.

Computation overhead: In KURCS, the cluster guard unicast key generation parameters to uncompromised cluster members, let K be the number of uncompromised cluster members, thus, to update the cluster key $2(K-1)$ encryption and decryption is carried out. In SKRR, the sink S send revocation message containing a list of revoked node and its nonce encrypted with the public key of the receiving node I, node I decrypt the received message and send an acknowledgement message comprising its nonce, encrypted with the public key of S back to S thus the computation overhead in respect of SKRR is $2(d-1).\ (d-1)$. The KMMR node revocation task involve each neighbor n deletes the shared PWKs shared with the compromised node, and at the same time update the LBKs. Suppose d as the number of uncompromised neighbours n , each neighbour n will carry out $(d-1)$ encryption and $(d-1)$ decryption operation. Sensor node in KeyRev scheme will compute t-degree polynomials in each of the revocation requests they received, encrypt every outgoing message, and also decryption and verification of the incoming messages.

Communication overhead: KURCS update of compromised key is carried out in the network, the cluster guard unicast key generation parameters to the uncompromised cluster members. SKRR, the revocation request is send by the sink S, an acknowledgment message is sent back to the sink S by the recipient R of the list, the recipient R send a new session key to it neighbour n, the neighbour n send a confirmation message back R to acknowledge the receipt of the new session key. In KMMR, two types of key are exchange in the protocol, the LBKs and the PWKs, each node broadcast a SPDM with it neighbor n in order to share it LBK, similarly, to share the PWKs, a SJRM is sent to each router by each node and a SRRM message is received in response. The KeyRev protocol communication cost is tied to the session key update of non-compromised sensor nodes in the network which is carried out in a single round broadcast of message to all nodes in the network.

Storage overhead: The storage requirement in SKRR demands that each sensor in the network store in its memory the public key of the BS, its own pair of public and private keys and a shared key with the sink prior to deployment, in the same manner, in KeyRev solution, each node of the network is loaded with the pre-distributed key materials and the personal secrets needed for the session key update process. To establish a secure network, the KMMR stores the following keys: LBK, PWK and GBK couple with a temporary key for its key distribution. In KURCS, three types of keys are stored in each sensor in the network, they include sensor-base station key, cluster key and sensor guard key.

TABLE IV. COMPARISON OF PERFORMANCE METRICS OF THE CENTRALIZED KEY REVOCATION PROTOCOLS

Protocol	Computation Overhead	Communication Overhead	Storage Overhead
KMMR	$2(d-1).(d-1) = 2(d-1)^2$ Enc/Dec	$2M(\ n_s, MAC_{PWK})$	4 keys + ID + n + Ts + Report
SKRR	$2(d-1).(d-1)\ Enc/Dec$	$2M(\ L, n_s\ , K'\ (I,R))$	5 Key + M + n_s
KURCS	$2(K-1)Enc/Dec$	2 M(IDs, L, TSt)	3 keys + R
KeyRev	Polynomials verification + session key	2t Polynomials + wIDs	3 keys + personal secret + NRL + n_s

V. CONCLUSION

Research on effective and low-cost key revocation protocol has received less attention. This work presents categories of key revocation protocols in WSNs with a focus on centralized key revocation protocols. The authors discuss and investigate the operational procedure of the selected centralized KR protocols: KMMR, SKRR, KURCS, and KeyRev, the study highlighted the performance, security strength and weakness of these protocols. Furthermore, these protocols were compared on the bases of security requirements of confidentiality, integrity, authenticity, and data availability as well as their performance in terms of computation, communication, and storage overheads. Consequently, this work addresses the assertion of no flawless protocols; hence, each protocol poses certain strengths and weakness and their feasibility for certain environments and applications. Therefore, this study provides a roadmap towards selecting and design of efficient key revocation protocols in WSNs. The authors intend as future work to further analyze and compare more protocols, implement and re-evaluate them on a uniform environment to perform the comparison.

REFERENCES

[1] Chinniah, P., & Krishnamoorthi, S. (2019). An Efficient Elliptic Curve based Key Management Scheme for Distributed Sensor Networks. European Journal of Engineering Research and Science, 4(6), 111-116.

[2] Mansour, I., Chalhoub, G., Lafourcade, P., & Delobel, F. (2014). Secure key renewal and revocation for Wireless Sensor Networks. In 39th Annual IEEE Conference on Local Computer Networks (pp. 382-385). IEEE.

[3] Mansour, I., Chalhoub, G., & Lafourcade, P. (2015). Key management in wireless sensor networks. Journal of sensor and actuator networks, 4(3), 251-273.

[4] Ge, M., Choo, K. K. R., Wu, H., & Yu, Y. (2016). Survey on key revocation mechanisms in wireless ensor networks. Journal of Network and Computer Applications, 63, 24-38.

[5] Eschenauer, L., & Gligor, V. D. (2002). A key-management scheme for distributed sensor networks. In Proceedings of the 9th ACM conference on Computer and communications security (pp. 41-47).

[6] Dini, G., & Savino, I. M. (2006). An efficient key revocation protocol for wireless sensor networks. In 2006 International Symposium on a World of Wireless, Mobile and Multimedia Networks (WoWMoM'06) (pp. 3-pp). IEEE.

[7] Wang, Y., Ramamurthy, B., & Zou, X. (2007). KeyRev: An efficient key revocation scheme for wireless sensor networks. In 2007 IEEE International Conference on Communications (pp. 1260-1265). IEEE.

[8] Wang, Y., Ramamurthy, B., & Xue, Y. (2008). A key management protocol for wireless sensor networks with multiple base stations. In 2008 IEEE International Conference on Communications (pp. 1625-1629). IEEE.

[9] Ge, M., & Choo, K. K. R. (2015). A novel hybrid key revocation scheme for wireless sensor networks. In International Conference on Network and System Security (pp. 462-475). Springer, Cham.

[10] Guermazi, A., Belghith, A., Abid, M., & Gannouni, S. (2017). KMMR: An Efficient and scalable Key Management Protocol to Secure Multi-Hop Communications in large scale Wireless Sensor Networks. KSII Transactions on Internet & Information Systems, 11(2).

[11] Mall, D., Konaté, K., & Pathan, A. S. K. (2013). On the key revocation schemes in wireless sensor networks. In 2013 IEEE International Conference on Green Computing and Communications and IEEE Internet of Things and IEEE Cyber, Physical and Social Computing (pp. 290-297). IEEE

[12] Vaid, R., & Kumar, V. (2015). KURCS: key updating for removing & replacement of compromised sensor nodes from wireless sensor networks. Int. Organ. Sci. Res. J. Comput. Eng. (IOSR-JCE), 17(3), 57-67.

[13] Ishmanov, F., Kim, S. W., & Nam, S. Y. (2015). A robust trust establishment scheme for wireless sensor networks. Sensors, 15(3), 7040-7061.

[14] D. Liu, P. Ning, and K. Sun, "Efficient self-healing group key distribution with revocation capability," in CCS '03: Proceedings of the 10th ACM conference on Computer and communications security. New York, NY, USA: ACM Press, 2003, pp. 231–240