American Journal of Advanced Research, 2019, 3–2
December. 2019, pages 1-6
doi: 10.5281/zenodo.3368588
http://www.ibii-us.org/Journals/AJAR/
ISBN 2572-8849 (Online), 2572-8830 (Print)

Peer to Peer Authentication for Index-based Distributed Data Collection: A Zero-Knowledge-based Scheme to Security for Wireless Sensor Networks

Aline Z. TSAGUE[1,2 *], Elie T. FUTE[1,2], Emmanuel TONYE[3] and Adnen EL AMRAOUI[4]

[1]Department of Computer Engineering, Faculty of Engineering and Technology, University of Buea, Buea, Cameroon,

[2]Department of Mathematics and Computer Science, Faculty of Science, University of Dschang, Dschang, Cameroon,

[3]Department of Electrical and Telecommunication Engineering, National Advanced School of Engineering, Yaounde, Cameroon,

[4] Laboratory of Computer Science and Automation of Artois, University of Artois, Artois, France

*Email: linetsague@yahoo.fr

Received on 06/05/2019; revised on 07/10/2019; published on 08/14/2019

Abstract

A primary concern of a wireless sensor network (WSN) is to gather data from the immediate environment of it sensors while minimizing the use of limited network and computational resources. Several studies have focused on how to efficiently store and process sensed data in WSN. Generally, the appropriate method to store sensed data depends on the application for which the WSN was deployed. No matter the application, data collection appears to be a primary function of a WSN. The execution of this function must be coordinated and effective in order to provide WSN with current security standards such as privacy, data integrity and end entity authentication between communicating peers. In this paper, we propose an efficient authentication-based security scheme for data retrieval in WSN. This security scheme combines zero-knowledge proofs (ZKP) and pre-shared key method to provide secured and authenticated communication during data retrieval by a mobile sink in WSN. The security mechanism proposed works on a clustered network topology with an index-based data dissemination scheme. The network employs the concept of Connected Dominating Set (CDS) to form storage and index node sets. Upon a successful peer authentication, the index, located on the index node, is used for efficient retrieval of data. The scheme also provides end-to-end confidentiality given that data is being encrypted before transferred and can be decrypted only at the base station. Security and performance analysis of the proposed scheme show that it addresses all of the aforementioned issues while also satisfying zero-knowledge proofs properties. It is also suitable for devices with limited computational resources as the network can fulfil the purpose of data collection and can be deployed in large-scale wireless sensor networks.

Keywords: Authentication, Data Collection, Dissemination, Distributed indexing, Security, WSN, ZKP

1 Introduction

Progress in the miniaturization of electronic components, combined with the standardization of wireless communications and the desire to improve the life quality of humans, led to the advent of wireless sensor network technology. A wireless sensor network (WSN) is composed of a collection of autonomous sensor nodes, interconnected via wireless links and deployed randomly on a geographically limited environment. Each of these nodes is capable of accomplishing tasks such as acquiring or capturing a physical quantity, possibly processing this data and communicating with other sensors and/or routing to a sink for analysis and decision making (Abdul et al., 2016; Aruna and Varalakshmi, 2013). The purpose of a WSN generally depends on the application for which it was deployed. However, its main goal is to gather a set of measures from the immediate environment of the sensors, such as temperature, radioactivity, CO2, or atmospheric pressure, in order to convey them to a processing station (Abdul et al., 2016; Wassim, 2010; Alsbouí et al., 2011; Krol, 2016). Wireless sensor networks (WSN) have been widely used over different domains for a variety of applications. No matter the application, data collection appears to be a primary function of a WSN. The execution of this function must be coordinated and effective in order to limit data redundancies and to reduce the number of communications that are very expensive in terms of energy consumed. It is therefore essential to be able to provide WSNs with an acceptable level of security, particularly with regard to the collection and proper routing of data to the base station. Trust is one of the major

concerns against such routing tasks. Indeed peers need to be sure with whom they are communicating and exchanging information. Provide P2P with current security standards: privacy, integrity and authentication between communicating peers. We need to establish of a trusted environment to address access control including identity verification, guarantee confidentiality and/or privacy of all content received over the network. Authentication refers to the process by which a peer (the prover, usually a user) provides some form of proof of his identity to another (the verifier usually the server) in order to access services/resources. Yet, the establishment of authentication between nodes in a peer-to-peer environment requires a bit more planning than in the typical client-server environment given that nodes (peers) are exchanging information directly with each other, instead of using some central stand-alone server.

The rest of the paper is organized as follows, section 2 presents conventional and current data collection techniques in WSNs and provides brief complexity analysis of the latter. Section 3 describes the basic idea of the CDS-based data dissemination scheme. In section 4 we present a brief overview of Zero Knowledge Proof (ZKP). Section 5 presents the proposed security scheme. Section 6 reports the conduct of our analysis of the proposed approach in order to evaluate its performance. Finally, section **7** concludes the work and gives future prospects.

2 Review of data collection approaches in WSNs

The development of a wide range of sensors, their low cost and the ability to deploy them at remote locations, have given a great run up for the use of WSN technology in a wide range of applications. Some of the application areas include environment and habitat monitoring, health, disaster and waste management, precision agriculture, transport and radiation detection. Conventional data collection methods in WSN involve the deployment of a large set of sensor nodes with the ability to sense specific events around their neighborhood and to communicate with adjacent neighbor nodes for onward transmission to a base station (Abdul et al., 2016). The captured data is then transmitted through several other sensor nodes in a multi-hop structure to a sink, then forwarded to the base station for processing and decision-making. This yields an important communication flow within the network, having as major consequence the depletion of the energy of sensors. It may also weaken the security strength (Aruna and Varalakshmi, 2013): some intermediate may modify the data passing by, capturing sensor nodes, launching a wormhole attack, a sybil attack, selective forwarding, sinkhole, etc. There are generally three components involved in the data collection process: the sensor nodes, the sink or collector and the processing station. Depending on the application requirement, the sink can be static or mobile (Abdul et al., 2016; Aruna and Varalakshmi, 2013; Francesco et al., 2011; Harchi, 2013). In case of static sink, nodes transmit their data to the sink from their respective positions while mobile sinks visit nodes to collect data. Then the sink also forwards the data to a base station for processing and analysis (Wassim, 2010; Alsbouí et al., 2011; Harchi, 2013). Given that the data collected is often intended to a target user community, the sink can act as gateway between the sensors and the final user to obtain information through queries.

Several studies have focused on how to efficiently store and process sensed data in WSN. Generally, the appropriate method to store sensed data depends on the application for which the WSN was deployed. There are three (03) main data dissemination approaches for data retrieval from WSNs (Ratnasamy et al., 2003; Noël, 2006; Le, 2008): external storage (ES) approach, local storage (LS) approach and data-centric storage (DCS) approach. The ES approach recommends that upon detection of events, the relevant data should be sent to an external storage where they are further processed as needed. This entails a cost of O(√n) for each event sent. There is no cost for external queries since the event information is already external. Nevertheless, the cost of updates transmission is high and the network's lifetime is not optimized for nodes at the vicinity of base station deplete their energy rapidly since they play two roles: sensing and routing messages from all other nodes. The LS approach recommends that event information is stored locally (at the detecting node) upon detection of an event; this incurs no communication costs. Nodes can avoid transmitting useless information to users. Yet, queries are flooded to all nodes at a cost of O(n). Only the nodes having the requested data can answer to a query. Responses are sent back to the source of the query at a cost of O(√n) each. There is a need for bigger storage space at long term. This model, just like the previous, also suffers from the absence of load balancing. The goal of DCS approach is to distribute data uniformly over the network. After an event has been detected the data are stored by name within the network. The communication cost to store the event is O(√n). Queries are directed to the node that stores events of that name, which returns a response, both at a cost of O(√n).

In order to provide low average query and storage communication and seek to balance those requirements over participating nodes, several other studies have investigated constructing an index and its variations to facilitate query processing in WSNs (Yiwei and Yingshu, 2009, Chao et al., 2011). It seems that any kind of index on distributed data requires a hierarchical structure to aggregate information from the whole network. More detailed information can be accessed by a top-down traversal of the hierarchy to visit the sensors holding the relevant information. This paper presents an efficient security scheme based on the DS-NIZKP presented in (Tsague, 2018) for data retrieval in WSN with an index-based data dissemination scheme during such visits. In the next section, we present the basic idea of the Connected Dominating Set (CDS)-based data dissemination scheme.

3 An index-based data dissemination scheme

CDS represents the network topology by a graph G = (V,E), where V is the node set and E is the edge set. If two nodes are within the transmission range of each other, then there is an edge between them (Yiwei and Yingshu, 2009; Chao et al., 2011; Asim et al., 2016). A Dominating Set S of G is defined as a subset of V such that each node in V \ S is adjacent to at least one node in S. A Connected Dominating Set (CDS) C of G is a dominating set of G which induces a connected subgraph of G. An example of CDS is illustrated on Figure 1.

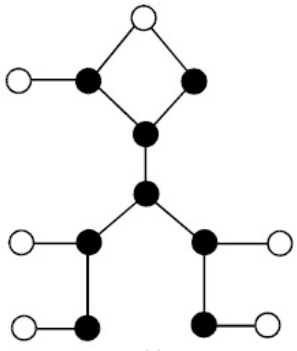

Fig. 1. An example of CDS, source (Gerardo, 2002)

The nodes in C are called dominators, the others are called dominatees. A k-hop dominating set D in G is a set of nodes with the property that every node in G is at most k hops away from at least one of the nodes of D. Figure 2 shows an example of 2-hop dominating set (DS), where black nodes represent dominators.

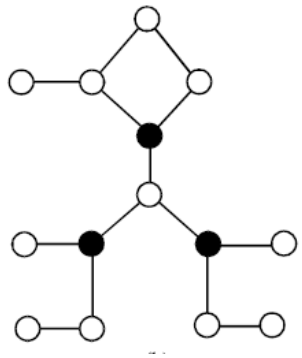

Fig. 2. An illustration of 2-hop DS, source (Gerardo, 2002)

In the CDS dissemination scheme, the network is logically divided into three layers as Figure 3 shows. The bottom layer contains the sensing nodes that monitor the targets and generate raw sensing data. The middle layer contains the storage nodes that are used to store the high level semantically rich data, which are derived from raw data and endowed with semantics so as to be understood easily. These nodes are close to the sensing nodes at a maximum distance of k-hop. The top layer contains the index nodes that store the index information for those high level semantically rich data. These nodes are determined by using a connected m-hop dominating set as index node set to dominate the storage nodes only.
Yet, storage nodes and index nodes in general consume more energy in handling various bypass traffic than sensing nodes. Those bypasses overhead will drain the energy of those storage nodes and index nodes very quickly. In order to prolong the life span of the whole network, authors in (Yiwei and Yingshu, 2009; Chao et al., 2011) propose that, the storage nodes and index do not need to do or at most do some part of sensing task. The authors in (Chao et al., 2011) further propose that each storage node should be equipped with standby node to reduce overload problem.

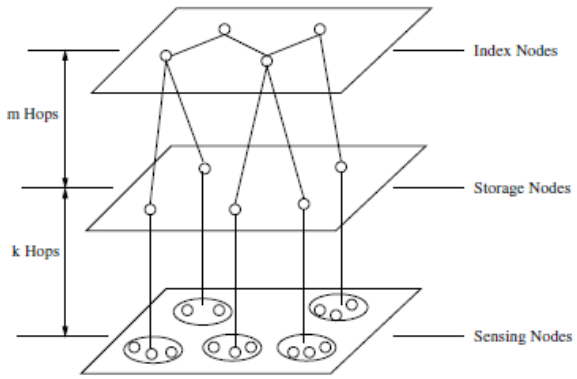

Fig. 3. Network hierarchy of CDS scheme, source (Gerardo, 2002)

4 Non-Interactive Zero-Knowledge Proofs (NIZKP)

A major concern during secured communications is to avoid any disclosure of sensitive information. Zero Knowledge Proof (ZKP) is an interactive protocol which enables one party (the prover) to demonstrate knowledge of a certain secret to another party (the verifier) without revealing any information about the secret itself. This protocol can be solved by using mathematical problems like random numbers, discrete logarithms and integer factorization (Gerardo, 2002; Kumar and Deepti, 2017) etc., to improve security. Typical ZKPs are based on several challenges and responses, involving a successive exchange of messages, which implies a very high communication cost. An extra consequence is the need to have a stable and continuous connection between nodes (Feige et al., 1988) so as avoid communication failure during the execution of the protocol. A ZKP must fulfill three main properties: completeness, soundness and zero-knowledge (Gerardo, 2002; Yu, 2012; Fernandez et al., 2016). Completeness means that for any valid input, a prover P can always complete the proof successfully (i.e. the verifier accepts the prover's claim). Soundness ensures that no malicious prover P can construct a valid proof system (i.e. the verifier can never been convinced by any prover if its claim is false). Zero-knowledge guarantees that no malicious verifier V is able to derive extra knowledge from the interaction (i.e. the verifier cannot learn anything except the fact).

The concept of Non-Interactive ZKP (NIZKP) (Yu, 2012; Fernandez et al., 2016; Blum et al., 1988; Rackoff and Simon, 1992) was later introduced to address the issue of successive exchange of messages in user authentication which has a non-negligible impact on the lifetime of the system in terms of resources usage. In an NIZKP, all of the challenges of a typical ZKP are condensed into a single package and sent in a single message (Fernandez et al., 2016). This results in considerably reducing the time necessary to exchange messages, given that only a single message is sufficient to verify user's identity. In this research, node authentication is performed via the DS-NIZKP (a NIZKP-based approach using Digital Signature) scheme presented in (Tsague, 2018). This approach employs digital signature with hash function to provide zero-knowledge and authentication of both the sender and message.

In the latter work, we use a general method for constructing signature out of length-restricted ones. The method consists of hashing a message/document into a short (fixed-length) string (using a SHA-3 algorithm), and applying the RSA signature scheme to the resulting hash-value. With the RSA approach, the message to be signed is input to a hash function that produces a secure hash value of fixed length. This hash value is then encrypted using the sender's private key to form the signature. Both the message and the signature are then transmitted. The recipient takes the message and produces a hash value. The recipient also decrypts the signature using the sender's public key. If the calculated hash code matches the decrypted signature, the signature is accepted as valid. Because only the sender knows the private key, only the sender could have produced a valid signature.

According to some studies, the computational overhead required for a peer to prove its identity can potentially be significantly less than that required for other approaches of authentication without the need for a trusted third party such as that of central server, while still remaining very difficult for an intruder to cheat (due to being based upon a NP problem for conventional implementations). Due to these characteristics, ZKPs were, upon their invention, immediately considered to be very well suited to providing security to resource-limited systems (e.g. smart cards) and these same characteristics make them a viable option for IoT small, e.g. resource constrained 8-32 bit embedded systems.

5 The Proposed Scheme

The proposed solution is designed to operate on hierarchical deployments consisting of a fixed number of interconnected devices with a mobile sink that moves to collect data from index nodes. It provides mutual

authentication for the communicating peers (sink and index nodes) by demonstrating knowledge of a secret information to each other without any disclosure of sensitive information. It also ensures the confidentiality and integrity of subsequent communications between the mobile sink, the index nodes and storage nodes by ciphering data before transmission.

Data collection in WSN highly depends on the structure of the network and the data dissemination scheme as described in section 2. The network can be flat or hierarchical (clustered) while the data dissemination scheme can be local, external or data centric storage. In this work, we consider that sensor nodes are organized in a three-layer hierarchical network topology as illustrated on Figure 3. It employs the CDS-based data dissemination scheme in which high level semantically rich data are stored on storage nodes while their related index information are stored on index nodes. Only the index nodes know where the corresponding information is found. Such dissemination schemes present the advantage of been costless in terms of energy consumption given that neither queries nor data are routed across the network. Data is stored by well designed nodes and collected by suitable mobile equipments such as a mobile sink. Within this configuration, data collection starts between the mobile sink and index nodes with whom they authenticate mutually, then between storage nodes and mobile sink after a successful authentication. Upon a successful peer authentication, the index, located on the index node, is used for efficient retrieval of data. Indeed, the index node can either redirect the communication to the corresponding storage node or get the information from the latter and transmit it to the sink.

We start by describing the pre-configuration stage where a pre-shared key method is used to generate and store a set of keys into the corresponding nodes. Next we present the identification stage during which nodes build solid and strong proofs to authenticate themselves to their peers for subsequent data collection and exchanges. These proofs are obtained based on cryptographic primitives such as hash function, digital signature scheme and encryption. Finally we present the verification stage where nodes verify the validity of authentication information of their peers and decide to grant them access or not.

5.1 The pre-configuration stage

This stage consists to establish the pre-shared keys to be used by peers for the authentication process. The pre-shared key method of authentication is used to enable a remote host to authenticate itself with a peer host by providing a secret key, which is known to both hosts. Any host that does not know the shared key cannot enter into negotiation. The key is pre-configured beforehand (eventually by the administrator), and is used to protect and authenticate data that flows during data collection. Peers maintain a list of all the remote hosts that are authorized to negotiate. This list contains the identity of the remote host and the pre-shared key known to that host.

Prior to deployment of the network, a couple of (Public key, Private key) pairs are generated. Any public key algorithm can be used, for example RSA (see the algorithm in table 1 below) or DSS. We denote.

PU = Public key and **PR** = Private key

On the one hand, for a given pair of keys (PU, PR), PU is stored specifically onto the index and storage nodes but could be stored basically into all nodes of the network. PU is accompanied by the identity of the corresponding mobile sink. It is possible to register a set of potential mobile sinks which will carry out the data collection task. On the other hand, H(PU) and PR are stored on the mobile sink, where H(PU) is the hash value of PU.

Table 1. The RSA key generation algorithm

ALGORITHM: RSA KEY GENERATION SCHEME
1. Choose two prime numbers, p and q */* private chosen Values*/*
2. Compute $n = p*q$ *// public calculated value*
3. Compute $\phi(n) = (p - 1)*(q - 1)$ */*public calculated value*/*
4. Find $\boldsymbol{e}$ such that e is relatively prime to $\phi(n)$ and less than $\phi(n)$; i.e. $\gcd(\phi(n), e) = 1$and $1 < e < \phi(n)$ *// public chosen value*
5. Determine $\boldsymbol{d}$ such that $\boldsymbol{d*e} \equiv 1 \pmod{\phi(n)}$ and $d < \phi(n)$ */* private calculated value*/*

The resulting keys are PU = (e, n) and PR = (d, n).

5.2 The identification stage

During this phase, peers wishing to enter into communication build solid and strong proofs to identify themselves to each other for subsequent data collection and exchanges. This is actually the first step that takes place in the authentication process itself. Since we have a mutual authentication each peer is both prover and verifier. Therefore each entity forms a proof to authenticate itself. Through their proofs, peers should be able to demonstrate to each other the possession and/or knowledge of a shared secret without revealing the secret itself. We accomplish this thanks to ZKP properties implemented using digital signature and hash function as in (Tsague, 2018).

The sink's proof is formed of 02 components:

- K = H(PU) : hash value of PU which was preloaded during the pre-configuration stage.
- Sign = E_{PR}(H(PU)) : digital signature of sink, can only be generated by the sink. Figure 4 illustrates the signature generation process. The input represents K=H(PU) whose value was preloaded at the pre-configuration stage.

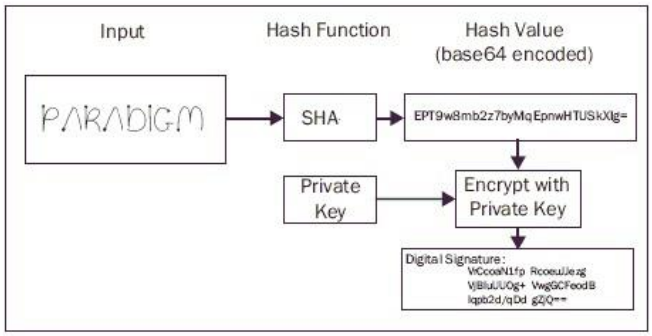

Fig. 4. Signature generation

The index node's proof consists of an acceptance message M, encrypted with PU, in case the sink is successfully authenticated.

5.3 The verification stage

The verification stage enables nodes to verify the validity of identification information of their peers and decide to grant them access or not. The verification of sink's information by index node proceeds as follows:

- Verification of sink's signature: decrypt Sign using the sink's public key and compare with H(PU). Figure 5 illustrates the signature verification process. After decrypting the signature received using te sink's public key, the index node can compute the hash value of this key then matches it with the decrypted information.
  - $S' = D_{PU}(Sign) = D_{PU}(E_{PR}(H(PU))$
  - $Cmp(S', H(PU)) = bool$

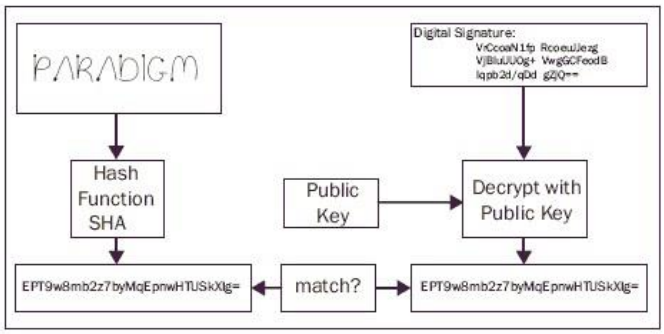

Fig. 5. Signature verification process

- Verification of sink's public key: compare K (the received information on the sink's public key) with the hash of the one stored on the index node H(PU).

On the other hand, the sink will receive an encrypted acceptance message with PU, EPU (M).

6 Security and Performance features

This section provides security analysis of the proposed solution in order to evaluate its performance. The security of the proposed solution mainly relies on the standards use to implement it: Zero-Knowledge Proof, Digital signature and Hash function. This section provides security analysis of the proposed solution in order to evaluate its performance. The security of the proposed solution mainly relies on the standards use to implement it: Zero-Knowledge Proof, Digital signature and Hash function. Let's start by evaluating the ZKP properties.

Completeness: this property guarantees that both the prover and the verifier will follow the normal protocol. For any valid K and signature Sign, the peers will accept and grant access with a probability very closed to 1 **Pr[V(K, Sign, P(K, Sign)) = 1] >= 1 –** $1/\epsilon$

Soundness: this property ensures that no malicious prover can construct a valid proof. A malicious node will not be able to cheat by sending an invalid key since it is not sent in clear form but hashed and signed using sink's private key **Pr[V(K, Sign, P'(K, Sign)) = 1] <** $1/\epsilon$

Zero-knowledge: this property refers that no information whatsoever except the validity of the prover's claim flows to the verifier. For any pair (K, Sign), no information is disclosed from K nor Sign to a third party that could affect user privacy thanks to hash functions properties.

The proposed solution satisfies completeness, soundness, and zero-knowledgeness properties of a ZKP. The security of the proposed scheme also depends on digital signature and hashing. Hashing (such as the SHA-3 family) algorithms provide special properties, such as resistance to collision, pre-image, and second pre-image attacks. These hash functions are also components for many important information security applications, including the generation and verification of digital signatures which have been used to implement the ZKP. Therefore, the proposal does not suffer from usual attacks based on cryptographic operations (also like identity theft and Man in the Middle attack), because its security is supported by NIZKP based on digital signature, current standard hashing and encryption.

7 Conclusion and Future works

In this paper we have proposed a security scheme to provide privacy, data integrity and end-entity authentication among peers in a static deployment of WSN, with an index-based data dissemination scheme. It is based on a zero-knowledge proof and has two unique features, e.g. it provides mutual authentication based on the use of digital signature scheme and hash function, while integrating a public key transport mechanism for a complementary key negotiation protocol.

The proposed solution provides perfect forward secrecy, but requires the distribution of credentials (e.g. public key components) pre-deployment, which becomes strenuous with large deployments. However, it avoids computational and management overheads created by alternative solutions that provide digital certificates and public key infrastructures in conventional IP networks.

Establishment of authentication between nodes in a peer-to-peer environment where nodes are exchanging information directly with each other requires more planning than in a typical client-server environment where the authentication methods are server-based. We are currently investigating the use of an alternative and lightweight key negotiating protocol based on elliptic curve Diffie–Hellman key agreement scheme (ECDH).

Acknowledgements

Thanks to Pr. Adnen El Amraoui for valuable documentation and support.

Funding

This work has not received any support by any organization.

Conflict of Interest: none declared.

References

Abdul Salaam G., A. Hanan Abdullah, M. H. Anisi, A. Gani and A. Alelaiwi (2016). A comparative analysis of energy conservation approaches in hybrid wireless sensor networks data collection protocols. In Telecommun Syst. Springer.

Alsbouí T. A. A., M. Hammoudeh, Z. Bandar, A. Nisbet (2011). An Overview and Classification of Approaches to Information Extraction in Wireless Sensor Networks. In The Fifth International Conference on Sensor Technologies and Applications (SENSORCOMM).

Aruna S. et Varalakshmi L. M. (2013). Data Gathering Using Sink Mobility with Three Tier Security Scheme in Wireless Sensor Network. International Journal of Engineering Research & Technology (IJERT), ISSN: 2278-0181, Vol. 2 Issue 12.

Asim Zeb et al. (2016), Clustering Analysis in Wireless Sensor Networks: The Ambit of Performance Metrics and Schemes Taxonomy.

Blum M., P. Feldman, S. Micali (1988). Non-interactive zero-knowledge and its applications, ACM Symp. Theory Comput. doi:10.1145/62212.62222.

Chao Gao et al. (2011), An efficient Index-based Data Storage Method for Wireless Sensor Networks. Information Technology Journal, Volume 10, ISSN 1812-5638.

Feige U., A. Fiat, A.Shamir (1988), Zero-knowledge proofs of identity. J. Cryptol, 1, pp 77–94.

Fernandez Martín F., P. Caballero-Gil and C. Caballero-Gil (2016), Authentication Based on Non-Interactive Zero-Knowledge Proofs for the Internet of Things, MDPI Journal Sensors, 16, 75, doi:10.3390/s16010075

Francesco M.D, S.K. Das and G. Anastasi (2011). Data Collection in Wireless Sensor Networks with Mobile Elements: A Survey. ACM Trans. Sen. Netw., 8(1).

Gerardo I. Simar (2002), A Primer on Zero Knowledge Protocols, Universidad Nacional del Sur.

Harchi S..(2013) Un protocole de session dans les réseaux de capteurs sans fils. Thèse de doctorat, Université de Lorraine.

Krol M. (2016), Routing in Wireless Sensor Networks. Thèse de doctorat, Université de Grenoble.

Kumar S. Mandal and A. R Deepti (2017). A General Approach of Authentication Scheme and its Comparative Study, International Journal of Computer (IJC).

Le H.-C. (2008). Optimisation d'accès au médium et stockage de données distribuées dans les réseaux de capteurs. Thèse de doctorat, Loctudy, Université de Franche-comté.

Noël G. (2006). Indexation dans les bases de données capteurs temps réel. Thèse de doctorat, L'Institut National des Sciences Appliquées de Lyon.

Rackoff C. and D.R. Simon (1992). Non-interactive zero-knowledge proof of knowledge and chosen ciphertext attack, In Advances in Cryptology, Feigenbaum, J., Ed.; Springer: Berlin, Gernamy. Volume 576, pp. 433–444

Ratnasamy S., B. Karp, S. Shenker, D. Estrin, R. Govindan, L. Yin, F. Yu (2003). Data-Centric Storage in Sensornets with GHT, a Geographic Hash Table. Mobile Networks and Applications 8, 427–442.

Tsague Aline Z. et al. (2018) "DS-NIZKP: A ZKP-based Strong Authentication using Digital Signature for Distributed Systems. International Journal of Computer Science and Information Security (IJCSIS), Vol. 16, No. 6.

Wassim Z. (2010). Quelques propositions de solutions pour la sécurité des réseaux de capteurs sans fil. Thèse de doctorat, Institut National des Sciences Appliquées de Lyon.

Yiwei Wu and Yingshu Li (2009). Distributed Indexing and Data Dissemination in Large Scale Wireless Sensor Networks. In Proceedings of 18th International Conference on Computer Communications and Networks.

Yu J. (2012), Remote user authentication in distributed networks and systems, Master's thesis, University of Wollongong.