SECURITY AND KEY MANAGEMENT CHALLENGES OVER WSN (A SURVEY)

Nesma Abd El-mawla[1], Mahmoud Badawy[2] and Hesham Arafat[3]

[1]Department of Communications and electronics, Nile Higher Institute for Engineering and Science, Egypt
[2,3]Department of Computers and systems Engineering, Mansoura University, Egypt

ABSTRACT

Wireless sensor networks (WSNs) have turned to be the backbone of most present-day information technology, which supports the service-oriented architecture in a major activity. Sensor nodes and its restricted and limited resources have been a real challenge because there's a great engagement with sensor nodes and Internet Of things (IoT). WSN is considered to be the base stone of IoT which has been widely used recently in too many applications like smart cities, industrial internet, connected cars, connected health care systems, smart grids, smart farming and it's widely used in both military and civilian applications now, such as monitoring of ambient conditions related to the environment, precious species and critical infrastructures. Secure communication and data transfer among the nodes are strongly needed due to the use of wireless technologies that are easy to eavesdrop, in order to steal its important information. However, is hard to achieve the desired performance of both WSNs and IoT and many critical issues about sensor networks are still open. The major research areas in WSN is going on hardware, operating system of WSN, localization, synchronization, deployment, architecture, programming models, data aggregation and dissemination, database querying, architecture, middleware, quality of service and security. In This paper we discuss in detail all about Wireless Sensor Networks, its classification, types, topologies, attack models and the nodes and all related issues and complications. We also preview too many challenges about sensor nodes and the proposed solutions till now and we make a spot ongoing research activities and issues that affect security and performance of Wireless Sensor Network as well. Then we discuss what's meant by security objectives, requirements and threat models. Finally, we make a spot on key management operations, goals, constraints, evaluation metrics, different encryption key types and dynamic key management schemes.

KEYWORDS

Wireless, sensor networks, WSN, challenges, issues, security.

1. INTRODUCTION

In Recent years, there are numerous advances in communication and wireless technologies. These advances lead to a new wireless networking generation which is called wireless sensor networks (WSN). WSNs gather sets of self-organized wireless ad hoc networks which consist of a large number of resource constrained sensor nodes. WSN facilitates the interaction between human and physical world. Present-day, human lives can be saved in wars with the data gathered by sensors, but WSNs in the near future will offer more surprises for humans as they come to be used in daily household matters like or controlling traffic in high-volume areas, locking doors and switching off electronics. For Example, sensors installed in big malls can guide people to their required products easily while those in forests provide immediate knowledge about disastrous hazards like wildfire and those in hospitals are responsible of monitoring patient condition and. These advantages are only a small fraction of what WSNs could potentially offer when deployed more commonly. Future studies can prove that WSNs are so useful in a wider variety of Applications.

DOI:10.5121/ijcses.2019.10102

The potential of Wireless Sensor Network is nothing short of revolutionary. Wireless sense and control technology is being developed to bridge the gap between the real world and the virtual world of electronics. This technology will affect all sides of our lives in the future. The dream is to automate every ting in life such as traffic, hospitals, forest fires, hurricanes and much more wide areas and with billions of sensors. So WSN is important to have open eyes on security issues of WSN and working hard to solve it.

Wireless sensor networks (WSN) mainly consists of many independent, *low-power*, low-cost devices capable of sensing, processing, and wireless communication. Their main purpose is to collect and disseminate environmental data and possibly perform some calculations. There has been a push, especially in industry, in recent years to make real-time data collected from WSNs more readily available to consumers of this information. However, there are no convenient tools or specific frameworks in place to allow instant access to this sensed information in a programming environment. Thus, one of the main problems with deploying WSNs is gathering the data they produce and using it in flexible ways. With the rapid technological development of sensors, WSNs will become the key technology for IoT.

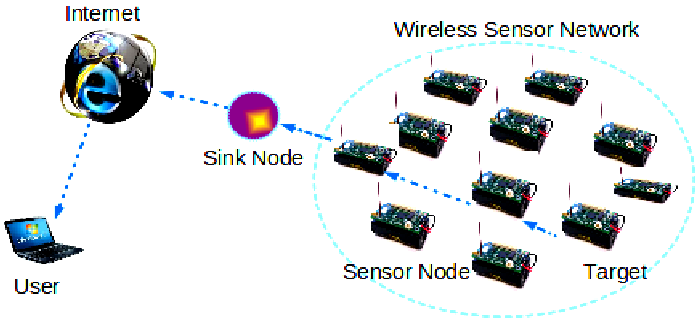

Figure 1. An example of wireless sensor network

The contribution of this paper is arranged as follows: in section 2, we present wireless networks, its elements, classification, overview on internet access in wireless networks, routers & battery powered routers. In section 3, we present an introduction to WSN, its applications, benefits, advantages & disadvantages. Also we present WSN types, topologies, limitations, open issues, challenges, security objectives and requirements, threat models and the attacks on WSN and why security is important. Section 4, presents background on key management operations as it's the main thing about security, stages, goals, constraints, and evaluation metrics. Section 5 introduces dynamic key management, related works and previous solutions. In section 6, the paper is concluded, and directions for future researches are outlined.

2. Wireless Sensor Networking

Wireless networks can be categorized due to the infrastructure into: (1) infrastructure mode (base station connects mobiles into wired network, handoff: mobile changes base station.) (2) Ad hoc mode (No wired) base stations (nodes can only transmit to other nodes within radio reach, nodes organize themselves into a network, route only among themselves) and due to its infrastructure of wireless networks we can classify it as the following:

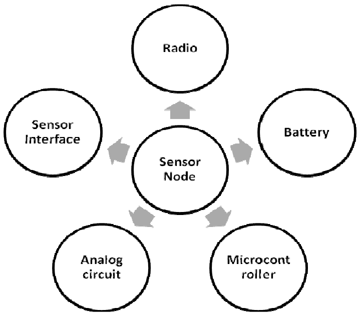

Figure 2. Wireless Sensor Node components

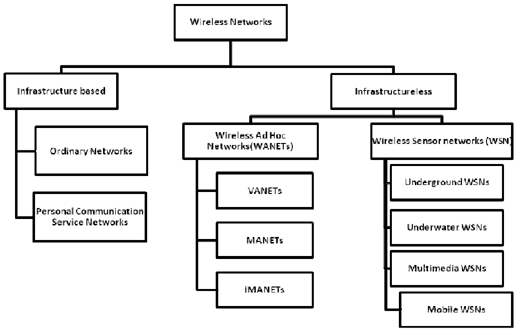

Figure 3. Wireless networks classification

2.1. WSN APPLICATIONS

A wireless sensor network (WSN) is a network formed by a large number of sensor nodes where each node is equipped with a sensor to detect physical phenomena such as light, heat, pressure, etc. WSNs are regarded as a revolutionary information gathering method to build the information and communication system which will greatly improve the reliability and efficiency of infrastructure systems. Compared with the wired solution, WSNs feature easier deployment and better flexibility of devices. With the rapid technological development of sensors, WSNs will become the key technology for IoT [6].
A Wireless Sensor Network (WSN) is by hundreds of small, low-cost nodes that are fitted with limitations in memory, energy, and processing capacity. In this particular form of networks, several problems are to learn each node. Recent advances in wireless communications and electronics have enabled the roll-out of low-cost, low-power and multi-functional sensors that are small in dimensions and communicate in a nutshell distances [7]. Nowadays there's too many Benefits of WSN. It's been used widely in many applications [8][9].It's used in Commercial building control, Environmental (land, air, sea) and agricultural wireless sensors, Home automation, including alarms (e.g., an alarm sensor that triggers a call to a security firm). National security applications: chemical, biological, radiological, and nuclear wireless sensors (sensors for toxic chemicals, explosives, and biological agents), Industrial monitoring and control, Metropolitan operations (traffic, automatic tolls, fire, etc.), Military sensors, Process control, Wireless automated meter reading and load management Observe.
WSN has many advantages and disadvantages which can be summarized as the following:

Table 1 - WSN advantages and disadvantages

Advantages	Disadvantages
Reduce Cost: Avoid a lot of Wiring.	**Speed:** Comparatively low speed of communication.
Easy Monitoring: It can be Accessed Through Centralized Monitor.	**Energy:** Life of Nodes & Energy Life.
Flexibility: to go through physical partition.	**Cost:** Costly at Large.
Extendable: can add new device any time.	**Security:** Easy For hacking.
Reduce Cost: Avoid a lot of Wiring.	**Disturbance**: get distracted by various elements.

2.2. WSN Types and Topologies

Wireless sensor networks topologies are classified based on number of hobs or power &transmission [10] [11], while types can be classified due to structure or use [8]. Due to structure, there are two types of WSN structure based or unstructured, different between two types is explained in (Table 1). Depending on the environment, the types of networks are decided so that those can be deployed underwater, underground, etc. Different types can be classified as Terrestrial, Underground, Underwater, Multimedia, and Mobile WSNs. The following figure explains different types and topologies of wireless sensor networks.

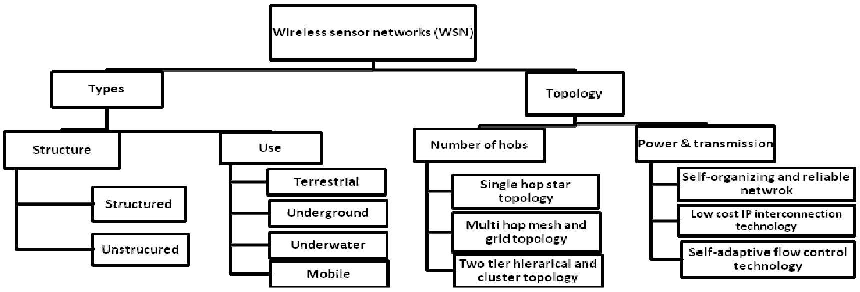
Wireless sensor networks (WSN)
Types
Topology
Structure
Use
Number of hobs
Power & transmission
Structured
Unstrucured
Terrestrial
Underground
Underwater
Mobile
Single hop star topology
Multi hop mesh and grid topology
Two tier hierarical and cluster topology
Self-organizing and reliable netwrok
Low cost IP interconnection technology
Self-adaptive flow control technology

Figure 4. WSN Types & Topology

Table 2. A comparison of structured and unstructured WSN

	Unstructured WSN	Structured WSN
Nodes	Dense Collection of nodes	Few and scarcely distributed nodes
Deployment	Ad-hoc deployment	Pre-planned Deployment
Maintenance	Difficulty in network maintenance	Lower Network Maintenance

2.3. OPEN RESEARCH CHALLENGES

Wireless sensor networks have many limitations due to sensor nodes as they are constrained by power, storage and processing capacity and thus require careful resource management. It also has insecure wireless communication due to the lack of infrastructure. Sensor nodes can be easily compromised and heterogeneous nature of sensor nodes makes a limitation. Frequent topology change due to nodes failures, joining or mobility makes a limitation. Classical IP-based protocols are not suitable because of the lack of global addressing scheme as well. A number of challenges and issues must be overcome for WSNs to become ubiquitous and used widely. These challenges can be summarized as shown in figure 5 [12][13][14][15].

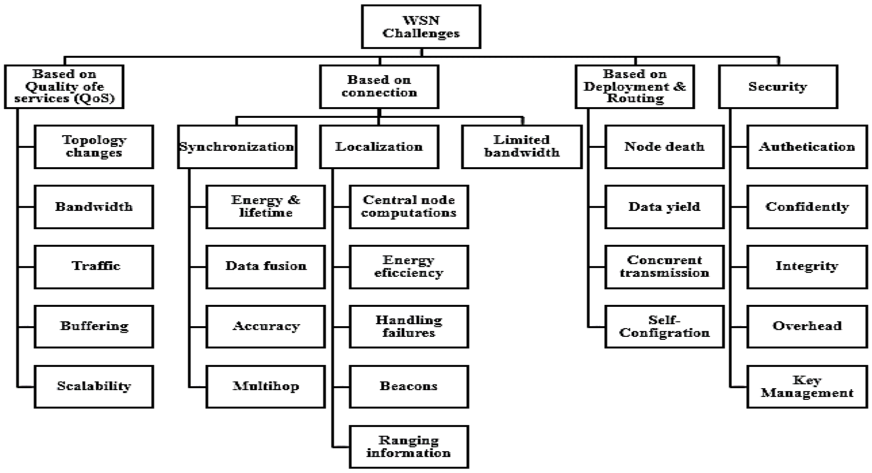

Figure 5-1. Challenges in WSN

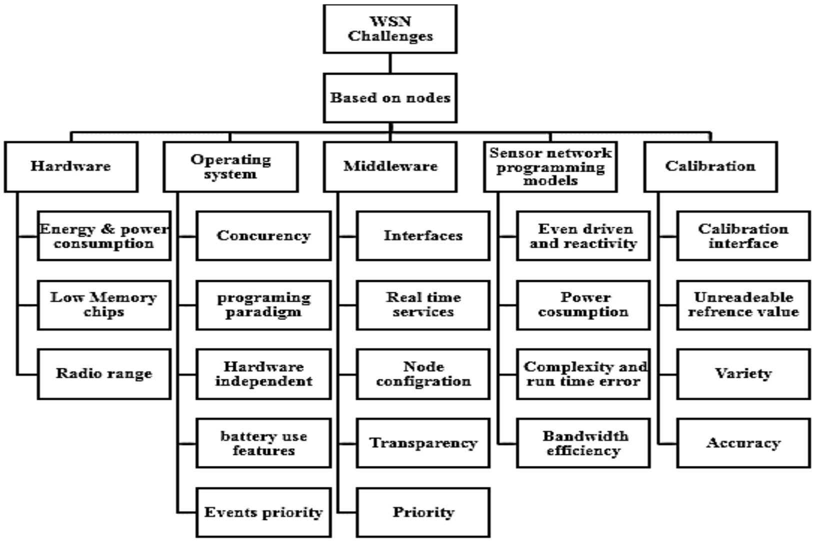

Figure 5-2. Challenges in WSN

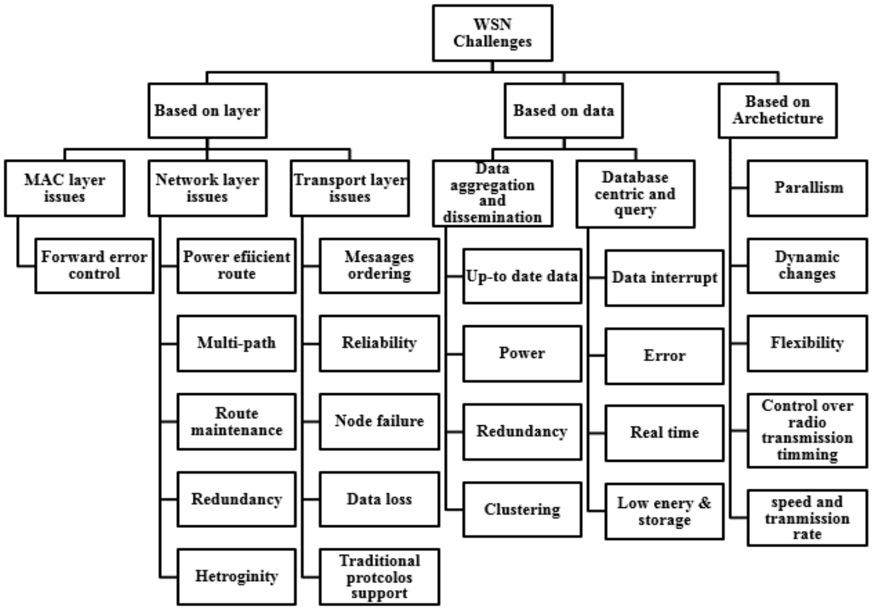

Figure 5-3. Challenges in WSN

And now, we will focus on most recent challenges and currently open issues in the environment that have effects on the performance of wireless sensor network.

1. **Interoperability:** Major three challenges in interoperability are of technical, semantic and pragmatic nature.
2. **Scalability:** sensing nodes are becoming large and unbounded so current WSN architectures need to be updated to cope up with the rapid growth of sensing nodes number. The current security protocol doesn't handle this growth as well, so it needs to be modified.
3. **Energy Efficiency:** sensors are limited due to energy, storage and life time so optimized, secure and efficient protocols need to be devised for WSN. A set of task need to be created

and find out each task which sensor is required, and for executing this task a sensor will be turned on sensor for particular time interval and after completion of task sensor will go to idle state. So, to improve energy efficiency of system. Efficient heterogeneous sensing of the urban environment needs to simultaneously meet competing demands of multiple sensing modalities. A generalized framework is required for data collection and modeling that effectively exploits spatial and temporal characteristics of the data, both in the sensing domain as well as the associated transform domains [48].

4. **Mobility Management:** current mobility protocols can't deal with mobile nodes efficiently due to energy and processing constraints, so mobility management is a critical point in WSN.

5. **Deployment:** Deployment means positioning and organizing an active sensor network in a real world environment. Nodes can be deployed by placing one after another in a sensor field or by dropping it from a plane. Deployment of sensor network is an intensive and cumbersome activity as we do not have influence over the quality of wireless communication and also the real world puts limitations and strains on sensor nodes by interfering during communications. Several deployment issues which need to be taken care are Power consumption and node death, Low data yield, Network Congestion & Self-configuration [16][17].

6. **Localization:** Sensor networks have been used in many fields like: object tracking, forecasting and distant control of dangerous regions, surveillance, and routing. In such applications, it is important for sensor data to be merged with location details. The location information of sensor can further help to assist routing in addition to calculating the coverage quality and attaining load balancing. Since sensor networks may be organized in unreachable environments or disaster assistance operations, the location of sensor nodes may not be schedule, so localization is one of the fundamental problems for many applications. It contains the identification and association of collected data, query and managing of nodes localized in a determined area, node addressing, coverage and nodes density evaluation, generation of energy map, topographical routing, object tracing, and other algorithms. The significance of localization data ascends from numerous factors, some of which are correlated only to WSNs. Hence, localization turnout to be a crucial research topic in WSNs. figure 6 summaries most of localization open issues [22][47].

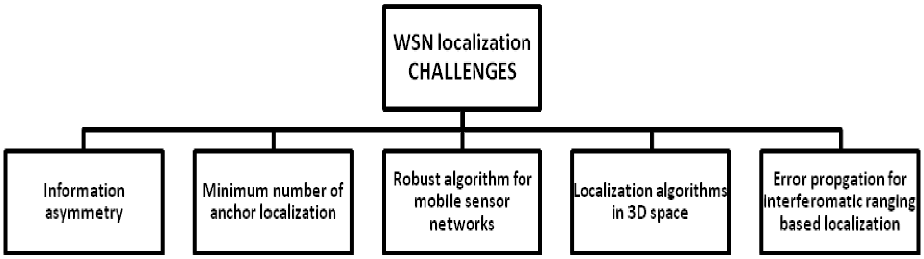
WSN localization CHALLENGES
Information asymmetry
Minimum number of anchor localization
Robust algorithm for mobile sensor networks
Localization algorithms in 3D space
Error propgation for Interferomatic ranging based localization

Figure 6. Taxonmy of Localization Open Issues

7. **Routing:** Routing in wireless sensor networks differs from classic routing in fixed networks in many ways. There is no infrastructure, wireless links are unreliable, sensor nodes may fail, and routing protocols have to meet strict energy saving requirements [27]. Many routing algorithms were developed for wireless networks in general. Here's a taxonomy of Routing Challenges & Design Issues [18][19]:

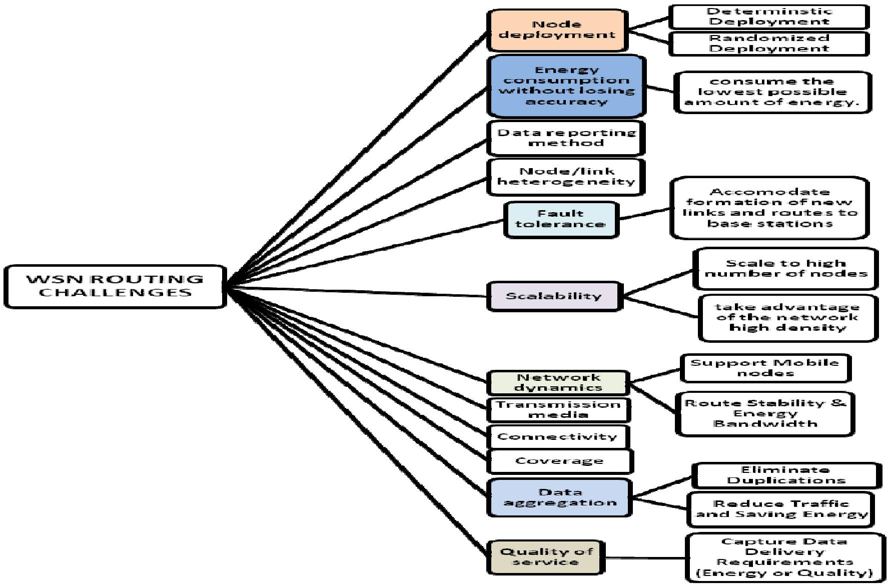
WSN ROUTING CHALLENGES
Node deployment
Determinstic Deployment
Randomized Deployment
Energy consumption without losing accuracy
consume the lowest possible amount of energy.
Data reporting method
Node/link heterogeneity
Fault tolerance
Accomodate formation of new links and routes to base stations
Scalability
Scale to high number of nodes
take advantage of the network high density
Network dynamics
Support Mobile nodes
Route Stability & Energy Bandwidth
Transmission media
Connectivity
Coverage
Data aggregation
Eliminate Duplications
Reduce Traffic and Saving Energy
Quality of service
Capture Data Delivery Requirements (Energy or Quality)

Figure 7. Taxonmy of WSN Routing Challenges & Design Issues

8. **Security:** Security is a broadly used term to include the characteristics of authentication, integrity, privacy, non repudiation, and anti-playback. The greater of the dependency on the info supplied by the networks may be increased, the more risk of secure transmission of information in the networks has increased. To the secure transmission of massive kinds of information over networks, several cryptographic, steganography and other techniques are utilized that happen to be used widely [20]. Following are the initial security requirements that every WSN application should adhere to [21]: Confidently, Authentication, Lack of Integrity, Protection against Message Reply Attack, Light weight Encryption Mechanisms & Secure Management and Key Distribution Techniques.

2.4. WSN Security Objectives And Requirements:

The aim of security services in wireless sensor networks is secure data against various types of attacks, so cryptography technique is so important for security services. There are many requirements for security services as listed below:

1. **Confidentiality**: hiding messages so that they can’t be understood by any unauthorized adversary.
2. **Authentication:** ability to identify reliability about the origin of the message.
3. **Integrity:** provides a mechanism to identify message tampering.
4. **Freshness and Availability:** guarantees the availability of network services to identify the movement of messages in the network. (If the nodes can use its resources, then availability is provided to the network for forwarding the message).
5. **Graceful Degradation:** network has performance graceful degradation when a small portion of nodes are compromised.
6. **Non-Repudiation:** sender and receiver shall not deny later about sending or receiving messages.
7. **Resiliency:** tolerate the attacks and continue offering its service uninterruptedly.
8. **Self-Healing:** ability of network to recover from security problems and isolate source of threat to stop the availability of network in future communications.

In brief, WSN main application is monitoring surroundings and returns the results to the sink node in a single or a multi hop. Each sensor node has sensing, memory, data processing and short-range radio communication unit. A sensor has limited computation, storage, energy resources and bandwidth. Wireless sensor network applications include target tracking, battlefield surveillance. They are deployed in hostile environments. Therefore the sensitive data should be protected well. An adversary snoop the traffic in a network and eavesdrop the secret messages. Secret keys are used to achieve data integrity and confidentiality. Communicating nodes authenticated and prevent the malicious node impersonating legitimate node for spreading wrong information. An adversary can inject packets, impersonate sensor nodes, provide misleading information and replay older messages. Therefore, security services are crucial. Key management is building block to provide such security services between communicating nodes.

2.5. Threat Models And The Attacks On WSN

Any WSN can be attacked or has many threats surround it; the major classification of threat models due to adversary enemy node is below:

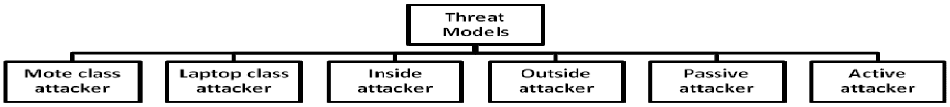

Figure 8. Threat Models of wireless sensor network

A (Mote class) attacker access only few motes in the network and (Laptop class) attacker access devices with more computational resources resulting in series attacks, while an (Inside attacker) can access the encryption keys or other codes in the network.
An (Outside attacker) is a passive listener to the network with no special access, while (Passive attacker) collects sensitive data from WSN and compromises the privacy. Active attacker disrupts the total network functionality and performance.
Most of WSN routing protocols are not designed to handle security issues, so that there are too many attacks on them can be categorized as Fooding attack, HELLO food attack, Black hole attack, Link withholding attack, Link Spoofing attack, Acknowledgement Spoofing attack, Replay attack, Wormhole attack, Colluding Mis-relay attack, Sybil attack, Sinkhole attack, Energy drain attack, Selective forwarding attack, Partition, Detour, Malign.

Many researches do their best to work on security challenges and issues of wireless sensor networks for Internet of thing applications. Here's a summarized view of some of their work:
A novel and secure privacy-enhanced mobile health-care scheme that is robust over the wireless cellular network is introduced by Baek et al. (2016) [35]. Their method considers real network environments and provides unlinkability between patient's alias and their real identification in all communication and satisfies the security requirements for mobile health-care systems as well.
Nguyen-Vu et al. (2016) [36] propose a practical scheme that dynamically secures and outsources data on demand, as well as introduce a corresponding architecture to securely process data in Database Service Provider. They also adopt the application of bring your own device (BYOD) in this scheme as an enhanced security solution.

A scheme to allow communication parties to change the security service flexibly without carrying out the datagram transport layer security (DTLS) handshake process each time under a resource constrained IoT environment is introduced by Ban et al. (2016) [37].

A security framework for the IoT environment that uses software-defined networking (SDN) technology is studied by Choi, S. and Kwak, J. (2016) [38]. They investigate strategies for establishing a security framework for the configuration of a software-defined IoT environment and efficient provision of security services. The service to decrease the overhead involved in security service provision is configured, and a simple test is conducted to verify the feasibility of the model.

3. BACKGROUND ON KEY MANAGEMENT OPERATIONS

Security solutions are depending very much on the use of strong and efficient key distribution and management. The key management mechanism is responsible for key generation, key distribution, and key maintenance among sensor nodes to establish and maintain secure channels. Key management should also allow sensor networks scaling to a large number of nodes. Key management stages are the set of operations as following:

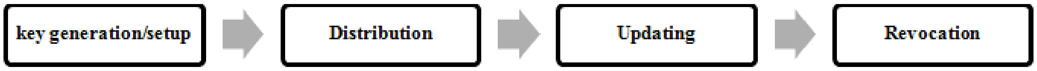

Figure 9. Key Management stages

Wireless sensor networks are operated on an unattended or disregarded mode. An adversary may physically capture sensor nodes to compromise their stored sensitive data and communication keys. Wireless sensors nodes are not attack resistant due to their low cost, so any adversary can get hold of a sensor node and can easily extract its stored cryptographic information. This attack is defined as node capture attack. Key protection, updating and revocation and are considered with special attention in wireless sensor networks. A number of key establishment protocols have been presented and proposed over the years. But these methods may not scalable well for large scale sensor networks which are deployed at different locations. They require massive amount of keying information to be pre-loaded into the sensor memory and thus storage space is wasted since much information may never be used during the sensor lifetime. They are also having more computation and communication overhead. They consume more energy. The current key management schemes need more messages transfer in key updating process.

3.1. KEY MANAGEMENT GOALS & CONSTRAINTS

To develop a key management protocol for any WSN the following goals must be achieved. The protocol must establish a key between all sensor nodes that must exchange data securely. It must support Node addition/ remove. It must work in undefined deployment environment as well and doesn't allow unauthorized to establish connection with network nodes. There are many constraints for achieving this as the process of securing WSN and developing a secure protocol is constrained by both network and nodes nature. Node Constraints as nodes in WSN have small memory, battery life time, processing capabilities and transmission range. And Network Constraints as WSN has mall packet size and ad-hoc nature and this constrained the cryptography process.

3.2. KEY MANAGEMENT EVALUATION METRICS

In order to evaluate different key management systems many metrics should be taken in consideration due to application nature [33][34].

- **Addition:** how complicated is dynamic node addition?
- **Revocation:** how complicated is dynamically node revocation?
- **Network Size:** what is the maximum possible size of the network?
- **Elasticity:** how many nodes are to be compromised in order to affect traffic of not compromised nodes?

4. DYNAMIC KEY MANAGEMENT

While there is a strong need to have secure internet connection for WSNs to ensure message confidentiality and there's many mechanisms to secure data while it's travelling between sensor nodes and hosts, but there's no such technique that guarantees a secure end to end (E2E) internet connection between sensor nodes and computer hosts with key distribution protocols on such resource constrained devices. Here are some old solutions of security & key distribution issue:

Table 3. A Comparison of three different Old Solutions for E2E security of WSN

	Proposed Solution	**Advantages**	**Disadvantages**
Securing communication with compressed IPsec [24]	Providing End-to-End (E2E) secure communication between IP enabled sensor networks and the traditional Internet. This is the first compressed lightweight design, implementation, and evaluation of 6LoWPAN extension for IPsec. Our extension supports both IPsec's Authentication Header (AH) and Encapsulation Security Payload (ESP). Thus, communication endpoints are able to authenticate, encrypt and check the integrity of messages using standardized and established IPv6 mechanisms.	- secure connection between sensor nodes and hosts. - No link layer security mechanisms so free some header space.	- The overhead of IPsec grows linearly with datagram sizes in multi-hops network.
Implementing IPsec with encapsulation security payload in wireless sensor networks [25]	The 6LoWPAN adaptation layer was extended to support both IPsec's Authentication Header (AH) and Encapsulation Security Payload (ESP). Thus, the communication endpoints in WSNs are able to communicate securely using encryption and authentication.	-End-to-end security in the emerging 'Internet of Things'. - System footprint under 16K bytes.	- No dynamic key distribution for the motes in the WSN-Internet communication network.
Key management for static wireless sensor networks [26]	A key management scheme for WSNs. It represents a new hybrid approach that integrates random seed distribution with transitory master key mechanisms. The main novelty of RSDTMK is the generation of pairwise keys based on randomly predistributed seeds, which are turned by a permutation function, and then are transformed in a key by a pseudorandom function, which employs a master key, deleted after a time-out period.	- Good connectivity and security features.	-Memory overhead. -Symmetric keys.

There were many disadvantages about these old Key Distribution Protocols due to huge amount of keying information to be pre-loaded into sensor's memory, Wasted storage space and communication overhead, more Computations over (memory, processing) and high energy consumption. Therefore it's a great need to new protocols for *Dynamic key management* and distribution processes.

4.1. Dynamic Key Management Schemes

Sensor network is easy node compromise, dynamic in structure, and self organized increased the difficulty of key management. Due to resources constraints such as power, memory, processing, and communication overhead the distribution and establishment of keys are a challenging task. There are two categories static and dynamic key management schemes. In static approach all keys are loaded to the sensor nodes and each node tries to get the shared keys of the neighbors. If a node can't discover a shared key, it can be setup with the assistance of one or more intermediate nodes. In dynamic approach some keys are loaded in sensor nodes previously and the session keys can be established by using these keys. Current Dynamic key distribution schemes can be classified as following [27][28][29]:

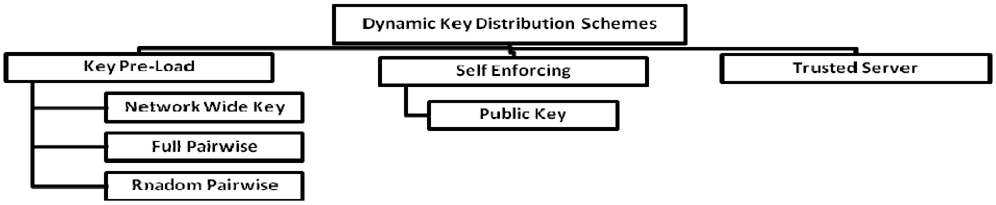

Figure 10. Dynamic Key Distribution Schemes

Table 4. A comparison of Different Dynamic Key Distribution Schemes

	Key Pre-load Distribution Schema			**Self Enforcing Scheme**	**Trusted Server Scheme**
	Network Wide Key	**Full Pairwise Keying**	**Random Pairwise Keys**	**Public Keys**	**-----**
Implementation	Simple	Simple	Simple	Complicated	**Based on Server Sink and Need Secure "Infrastructure", so it doesn't suitable for wireless sensor Networks**
Storage overhead	Low	High	Low	High	
Computations overhead	Low	Low	Medium	High	
Memory overhead	Low	Low	Medium	High	
Energy consumption	Low	Low	Medium	High	
Communication overhead	---	---	---	No	
Symmetric or Asymmetric key	Symmetric	Symmetric	Symmetric	Asymmetric	
Secure	No	Yes	Yes	Yes - High	
Scalable	Yes	No	No	yes	

Table 5. A Comparison of Symmetric and Asymmetric Key

	Symmetric Keys	**Asymmetric Keys**
Advantages	Efficient Key Management Low-Medium Overhead	Increase Network Security
Disadvantages	Less Security	Memory Overhead Energy consumption More computations

4.2. PREVIOUS PROPOSED SOLUTIONS

Many researchers produced various solutions but more security features are needed and many work to do in the future. Here's an overview of previous proposed solutions:

Sahingoz and O.K. (2013) [27] propose a practical key management framework for a large-scale distributed wireless sensor network system is presented. WSN nodes constitute a group and securely communicate with each other by symmetric encryption. As a structure of the mechanisms, this group key should be refreshed in certain intervals by help of UAVs and a more secure encryption mechanism; asymmetric encryption.

An attack model based highly secure management scheme developed by Ahlawat, P. and Dave, M. (2018) [33] to reduce the node capture impact for cellular model of WSN. The adversarial model exploits several vulnerabilities present in the network such as high node density, placement of the sink node, neighbor influence factor to compute the compromise probability of each cell. It then defines the hash chain length for each cell with different rekey interval to increase the network resistance against node capture attack. The proposed scheme is compared with other existing schemes in terms of the probability of key compromise and the number of links rekeyed. The results confirm its effectiveness in increasing the WSN security.

Sahingoz and O.K. (2013) [28] propose a practical key management framework for large-scale distributed WSN system based on sharing key between nodes mutually and asymmetric key encryption is used with the help of UAVs. The proposed system improves the efficiency of the system by decreasing the overhead such as storage and computations and by increasing network lifetime.

A a scheme on large-scale sensor networks based on executing the algorithm for public keys distribution and updating on MA and only cluster head sensors are responsible for key generation and distribution which help to save resources in normal sensors and this is good only if neighboring sensors. The scheme proposed by Kuchipudi et al.(2016) [29].

Du et al. (2007) [30] and Mungara et. al. (2012) [31] contemplate the key management process in a Heterogeneous Sensor Network (HSN) that consists of a small number of powerful High-end sensors (H-sensors, e.g., PDAs) and a large number of Low-end sensors (L-sensors, e.g., the MICA2-DOT nodes) .

A basic key management protocol based on initial secure time, which assumes that the attacker cannot compromise a node in a short time proposed by Cui et al. (2015) . It satisfies various security requirements of WSNs using the combination of four kinds of secure keys. Meanwhile, the erasure and update mechanism of keys is important to support network security. It's such a good proposal for key establishment and achieves security mainly based on the combining application of four kinds of keys. This is a critical step and how to use such keys to found a protection mechanism.

A system supports users full private key's combination of a partial non-public key generating by a Key Generation Center (KGC) and therefore the users secret price by Seo et al. (2015) [42]. Special Organization of the complete private/public key combine removes the requirement for certificate. Effective sharing between 2 nodes while not requiring onerous pairing operations and therefore the exchange of certificate.

Vasala et al. (2017) [43] propose a system with Users full private key's combination of a partial non-public key generating by a Key Generation Center (KGC) and therefore the user's secret price. Supports special organization of the complete private/public key combine removes the

Requirement for the certificate an effective sharing between 2 nodes while not requiring onerous pairing operations and therefore the exchange of certificate. They present a certificate-less effective key management (CL-EKM) scheme for dynamic WSNs.

A series of solutions and methods to achieve confidentiality with end-to-end guarantees, by using group-based keys within the context of a clustered and distributed key management framework. These solutions proposed by Esposito et al. (2018) [46]. They have implemented such solutions on top of TinyOS, and assessed their achievable quality by means of the TOSSIM simulator.

A new scheme for dynamic wireless sensor network was proposed by Goyal et al. (2012) [44] which enable establishing secure links between any two SNs located within their communication range. The novelty of this new scheme is that, no need for storing the keys in a key pool because the keys are generated randomly after deployment of nodes. Master key is generated by applying pseudo random function on one of initial key that is generated for that particular node. At different time, different initial keys are generated so adversary can-not get any key information during establishment. It removes the node addition attack, node cloning attack, HELLO flood attack and also increases the security within cluster by introducing cluster key.

Chen et al. (2008) [45] propose a dynamic key management scheme. This scheme can achieve a dynamic key management to prevent the replay attack via using GPS technology to find the nearest node of the BS to the neighbor cluster nodes. They also propose a nonce-based mechanism to complete the mutual authentication between the BS and cluster nodes. It can enhance the information security. They coped with the storage and energy consumption limitations and reduced the computation cost of the sensors.

Kumar, V. (2018) [50] introduced an improved key management scheme supporting node mobility in heterogeneous sensor networks. He used the concept of hash collision keys to improve the key sharing probability between the nodes. It increases the connectivity without increasing key size of key ring. Results of the proposed scheme are compared with the Sarmad-scheme [62] and basic scheme [59] in terms of various evaluation metrics. Results show that proposed scheme gives better network resilience and connectivity, while increasing an insignificant computation and storage overhead.

Zhang, Q. et al. (2018) [51] propose a key establish protocol for the WSNs based on combined key. The protocol adopts seed key mapping technology to achieve two-party and multi-party key establish in the WSNs, it can generate a large number of combination keys with little resources. So it effectively solve the contradiction between the sensor nodes need large storage space to store shared key with their neighbors and their limited storage space. It can also achieve mutual authentication between nodes when they establish shared key. Analysis shows that the proposed protocol has the advantages in storage efficiency, computation consumption and Communication consumption and suitable for wireless networks.

Mall, D. et al. (2017) [52] address the optimization problem of CL-EKM protocol [60]. Our enhanced scheme successfully reduces the energy cost associated with the communications from the BS to all cluster head nodes, makes the original protocol more delay efficient, offers higher flexibility, and scalability. Also, their scheme offers a cost effective solution. As a future work, the case of multiple base stations and specific application oriented WSNs could be taken into consideration to assess the efficiency of the enhanced mechanism.

An efficient dynamic authentication and key distribution scheme was proposed for heterogeneous WSN by Athmani, S. et al. (2017) [53]. The proposed protocol not just meets the prerequisite of confirmation and key administration for heterogeneous sensor arrange, yet additionally upgrades memory utilization, reduces computation complexity and communication overhead which improves the energy efficiency. The key distribution algorithm is based on pre-existing information to create dynamic keys and does not require any secure channel and sharing phase which confirms the obtained experimental results in terms of performance enhancement compared to related works. Also EDAK is more scalable and flexible for its application to large networks. Figure 11 shows the used data packet format and the sequence of the key establishment process.

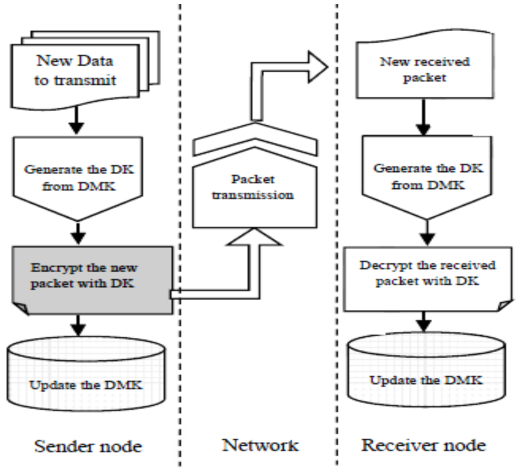

Figure 11. Data Packet Format & Key Establishment Process

For future work, they plan to extend their protocol to address other security issues including freshness and data integrity.

Kamble, S.B. and Jog, V.V., (2017) [54] presented the CSC scheme which provides a way to securely exchange and manage keys in wireless sensor networks. This solution easily accommodates for a dynamic environment where nodes will enter and leave the network. They showed the performance of their proposed scheme in terms of energy consumption and provided a discussion how their scheme can help the network in overcoming different attacks. In the future, they are planning to provide more comparisons considering the security and the resource consumption aspects to show the performance of the networks with their proposed scheme.
Existing data security solutions cannot be applied in such applications as they cannot deal with data streams with high-volume and high-velocity data in real time. Puthal, D. et al. (2017) [55] introduce a significant buffering delay during security verification, resulting in a requirement for a large buffer size for the stream processing server. To address this problem, they propose a Dynamic Key-Length-Based Security Framework (DLSeF) based on a shared key derived from synchronized prime numbers; the key is dynamically updated at short intervals to thwart potential attacks to ensure end-to-end security. Theoretical analyses and experimental results of the DLSeF framework show that it can significantly improve the efficiency of processing stream data by reducing the security verification time and buffer usage without compromising security.

Efficient key management technique is designed for implementing security mechanism by key authentication scheme along with energy efficient packet transmission in WSN. In secure WSN efficiency is measured by maximization of throughput by decreasing packet loss ratio and enhancing packet delivery ratio in network. This management technique was designed by Kandah, F.I et al. (2017) [56]. Figure 12 shows the proposed system architecture. This system designs certificate-less key management technique for secure key management. A CL-EKM supports efficient key updating when a new node connects a cluster also provide the key secrecy. This scheme is flexible against node copy, compromise, and network attacks. It secures the data confidentiality as well as data integrity. An experimental result shows the efficient routing for efficient packet transmission using four types of keys. Keys play important role in sensor nodes authorization authentication in wireless network communication. In this system the proposed effective key management technique helps to improve the security and energy efficiency of wireless network. Proposed algorithm computes for maximizing throughput by reducing overhead of sensor node with shortest path algorithm. It computes throughput by minimizing packet drop ratio. For future work, they are planning to work on energy consumption, based on CL-EKM for efficient packet transmission with various parameters related to node movements.

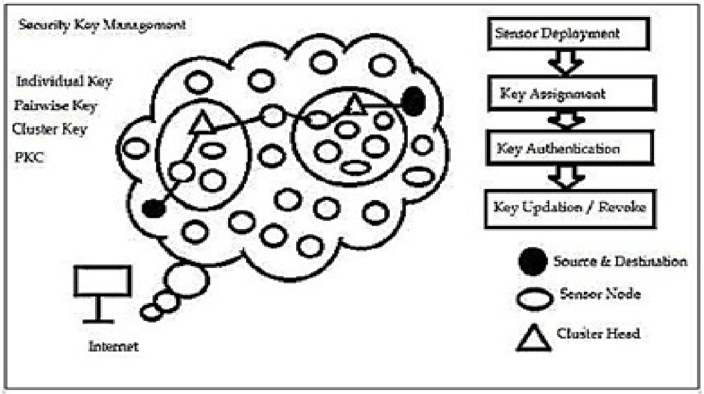

Figure 12. System architecture of Security management

Mahmood, Z. et al. (2017) [57] proposed an Efficient Keying for Multi-party (EKM) scheme to calculate the polynomial values using lightweight XOR operations. Pre-deployment, node joining, and key establishment protocols are also included. Before the nodes' deployment in WSNs, each sensor node is pre-configured with a set of symmetric keys shared with all the other sensor nodes of the network to transmit IDs securely. After the network deployment, every sensor node identifies the specified symmetric keys used to communicate with the cluster head (CH). The cluster-head maintains all the symmetric keys shared with the sensor nodes belonging to its cluster. The main reason the use of these symmetric keys is to facilitate the multi-hop communication while transmitting secret data, particularly, the personal-proportion distribution and the exchanged facts among the cluster-heads and the base station (BS). An intra-group key which derived from the implementation of the polynomial can reduce the session key storage overhead at the member nodes and their CH. After the intra-group key is acquired, the member nodes self-generate the polynomial functions, which are necessary for growing an inter-organization key. This show why the communication overhead on the CH is reduced. They have proposed a key generation and update mechanism for secure data sharing in identical clusters and among different cluster. In the session key generation mechanism for intra-clusters, the proposed technique significantly decreases the number of broadcast messages in the inter-cluster communication. The extra number of re-keying messages and communication overheads due to the proposed scheme has been conscientiously justified. Through the usage of the proposed mechanism, there's a great improvement to the WSN efficiency and network lifetime by reducing the number of exchanged messages to enhance the network lifetime during node mobility while reducing the coverage area of cluster heads and the need to migrate nodes to join the powerful coverage area of the CH. This research introduces a secure node migration protocol in which reliable handoff occurs and new connections are established between CHs and member nodes.

Yagan, O. and Makowski, A.M. (2016) [58] investigate the resiliency of wireless sensor networks against sensor capture attacks when the network uses the random pairwise key distribution scheme of Chan et al. they introduce conditions on the model parameters so that the network is:

1) unassailable and 2) unsplittable, both with high probability, as the number n of sensor nodes becomes large. Both notions are well defined against an adversary who has full knowledge of the network topology and unlimited computing resources, but can only capture a negligible fraction o(n) of sensors. They also illustrate that the number of cryptographic keys needed to ensure unassailability and unsplittability under the pairwise key predistribution scheme is an order of magnitude smaller than it is under the key predistribution scheme of Eschenauer and Gligor. The pairwise scheme and its induced random graph are parametrized by two positive integers n and K such that K <n. The network comprises n nodes, labeled i = 1, . . . , n, with unique ids Id1, . . . , Idn. Write Nn = {1, . . . , n} andset Nn,−i = Nn −{i} for each i = 1, . . . , n. With node i, we associate a subset Γn,i(K) of K nodes selected uniformly at random from Nn,−i – Each of the nodes in Γn,i(K) is said to be paired to node i. Thus, for any subset A ⊆ Nn,−i. The introduced model can be summarized as shown below in figure 13.

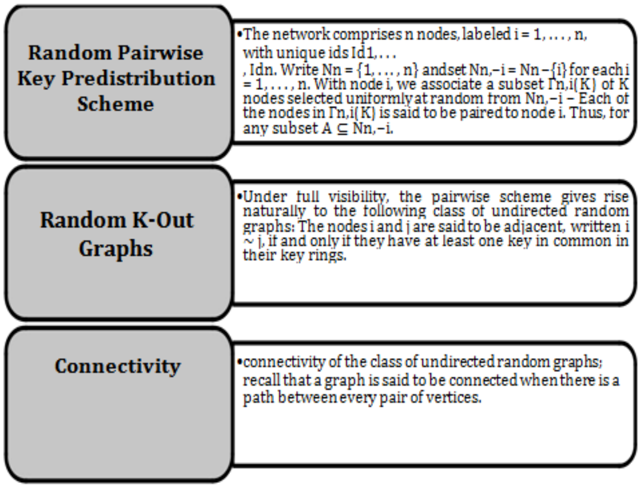
Random Pairwise Key Predistribution Scheme
•The network comprises n nodes, labeled i = 1, . . . , n, with unique ids Id1, . . . , Idn. Write Nn = {1, . . . , n} andset Nn,−i = Nn −{i} for each i = 1, . . . , n. With node i, we associate a subset Γn,i(K) of K nodes selected uniformly at random from Nn,−i – Each of the nodes in Γn,i(K) is said to be paired to node i. Thus, for any subset A ⊆ Nn,−i.
Random K-Out Graphs
•Under full visibility, the pairwise scheme gives rise naturally to the following class of undirected random graphs: The nodes i and j are said to be adjacent, written i ~ j, if and only if they have at least one key in common in their key rings.
Connectivity
•connectivity of the class of undirected random graphs; recall that a graph is said to be connected when there is a path between every pair of vertices.

Figure 13. Presented Model Overview

This work can be extended in several directions. Firstly, the analysis of the resiliency properties of sensor networks has only been done under the full visibility assumption. Future research should address situations where wireless communication connectivity is explicitly taken into account. Secondly, it might be worthwhile extending the analysis to key pre-distribution schemes other than the EG scheme and the pairwise scheme. A good candidate would be the q-composite scheme introduced in [61], which is a direct extension of the EG scheme. Finally, one might revisit the analysis with a less powerful attacker model and examine how the required key ring sizes are affected by the capabilities of the potential adversary.

Table 6. A briefing table of security& Key management related work

	Paper Title	Major Challenge	Main Characteristics & Future Work
1	ECL-EKM: An enhanced Certificateless Effective Key Management protocol for dynamic WSN	**Dynamic Key Management in WSN**	1. Public key based scheme to reduce energy cost. 2. Multiple base stations and specific application oriented WSNs could be taken into consideration.
2	EDAK: An Efficient Dynamic Authentication and Key Management Mechanism for heterogeneous WSNs		1. Light weight authentication algorithm. 2. Dynamic allocation algorithm. 3. It needs to be extended to include data integrity and freshness.

3	Efficient key management for dynamic wireless sensor network		1. Public/Private key technique. 2. Reduces overhead of sensor nodes using shortest path algorithm.
4	DLSeF: A dynamic key-length-based efficient real-time security verification model for big data stream		1. Symmetric key Cryptography. 2. dynamic key and dynamic key length as well. 3. It needs to be developed to work with Big Data streams and moving toward IoT.
5	Efficient key management for Big Data gathering in dynamic sensor networks		4. Dynamic environment where nodes enter and leaves the network. 5. It needs more comparisons according to security and resources consumption.
6	A Polynomial Subset-Based Efficient Multi-Party Key Management System for Lightweight Device Networks		1. Based on clustering technique. 2. Reduces energy consumptions with XOR than polynomial calculations. 3. It will be extended to be Ubiquitous to IoT.
7	Improving Key Management Scheme Supporting Node Mobility in Heterogeneous Sensor Networks using Collision Keys.		1. Hash collisions key technology. 2. Further it will need to improve the performance not connectivity only. 3. It needs to be simulated and try mobile sinks.
8	An Authentication Key Establish Protocol for WSNs Based on Combined Key		1. Combination keys and key mapping technology. 2. Fit for large scale WSNs.

5. CONCLUSION

Security & Key management for WSNs is a critical research point that has been addressed through many proposed schemes presented in different papers. This paper presents an overview of these techniques and solutions each of which offers different advantages and disadvantages. Both requirements and resources of a WSN determines which key management scheme should be employed as well. It gives attention to dynamic key management, its requirements and its evaluation metrics. Decisions regarding the key management scheme to be used must be based on these requirements for efficiency. The study of dynamic key management in wireless sensor networks still has abundant research opportunities in the future. As systems become more diminutive, more puissant, and use less energy, the security restraints will become more complex. Up to now, key management systems are a trade-off of performance and security to achieve low over head in memory usage and message transmissions. Key management systems sole purpose is to supply secure communication in wireless sensor networks without producing much overhead. More schemes should be developed to make efficient use of sensor nodes' limited resources [39][40][41]. More attention, study and work should be given to the security in key management schemes. Future research should especially seek techniques for using asymmetric dynamic key management techniques with low resources overhead, power consumption, low communication overhead and could handle new sensor nodes and different threat models as well.

ACKNOWLEDGEMENTS

We would like to thank our colleagues who provided insight and expertise that greatly assisted the research. We also feel grateful to Nile Higher Institute for Engineering & Technology managers as this work was supported in part by them.

REFERENCES

[1] "Overview of Wireless Communications". Cambridge.org. Retrieved 8 February 2008.

[2] Aravamudhan, L., Faccin, S., Mononen, R., Patil, B., Saifullah, Y., Sharma, S. and Sreemanthula, S., 2003. Getting to know wireless networks and technology. InformIT 2009.

[3] Fouchal, S., Monnet, Q., Mansouri, D., Mokdad, L. and Ioualalen, M., 2012, July. A new clustering algorithm for wireless sensor networks. In Proceedings of the seventeenth IEEE Symposium on Computers and Communications (ISCC'12), Nevsehir, Turkey.

[4] Miao, G., Zander, J., Sung, K.W. and Slimane, S.B., 2016. Fundamentals of Mobile Data Networks. Cambridge University Press.

[5] Kerr, Dana. "Google said to deploy Wi-Fi blimps in Africa and Asia". Archived from the original on 2017-03-14.

[6] Raza, S., Duquennoy, S., Chung, T., Yazar, D., Voigt, T. and Roedig, U., 2011, June. Securing communication in 6LoWPAN with compressed IPsec. In Distributed Computing in Sensor Systems and Workshops (DCOSS), 2011 International Conference on (pp. 1-8). IEEE.

[7] Varadarajan, P. and Crosby, G., 2014, March. Implementing IPsec in wireless sensor networks. In New Technologies, Mobility and Security (NTMS), 2014 6th International Conference on (pp. 1-5). IEEE.

[8] Pfeifer, T., Olariu, S. and Fersha, A., 2005. Wireless sensor networks and their applications. special issue of Computer Communications, 28.

[9] Sohraby, K., Minoli, D. and Znati, T., 2007. Wireless sensor networks: technology, protocols, and applications. John Wiley & Sons.

[10] Sharma, D., Verma, S. and Sharma, K., 2013. Network topologies in wireless sensor networks: a review 1.

[11] Kaur, G. and Garg, R.M., 2012. Energy efficient topologies for wireless sensor networks. International Journal of Distributed and Parallel Systems, 3(5), p.179.

[12] Karthik, S. and Kumar, A.A., 2015, March. Challenges of Wireless Sensor Networks and Issues associated with Time Synchronization. In Proceedings of the UGC Sponsored National Conference on Advanced Networking and Applications.

[13] Gupta, K. and Sikka, V., 2015. Design Issues and Challenges in Wireless Sensor Networks. International Journal of Computer Applications, 112(4).

[14] Sharma, S., Bansal, R.K. and Bansal, S., 2013, December. Issues and challenges in wireless sensor networks. In Machine Intelligence and Research Advancement (ICMIRA), 2013 International Conference on (pp. 58-62). IEEE.

[15] Romer, K. and Mattern, F., 2004. The design space of wireless sensor networks. IEEE wireless communications, 11(6), pp.54-61.

[16] MartíNez, J.F., Familiar, M.S., Corredor, I., GarcíA, A.B., Bravo, S. and LóPez, L., 2011. Composition and deployment of e-Health services over Wireless Sensor Networks. Mathematical and Computer Modelling, 53(3), pp.485-503.

[17] Li, J., Bai, Y., Ji, H., Ma, J., Tian, Y. and Qian, D., 2006, October. Power: Planning and deployment platform for wireless sensor networks. In Grid and Cooperative Computing Workshops, 2006. GCCW'06. Fifth International Conference on (pp. 432-436). IEEE.

[18] Mehndiratta, N. and Bedi, H., 2013. Design Issues for Routing Protocols in WSNs Based on Classification. International Journal of Application or Innovation in Engineering & Management (IJAIEM), 20, p.13.

[19] Deshwal, T. and Verma, P., Routing Challenges in WSN (Wireless Sensor Networks).

[20] Pathan, A.S.K., Lee, H.W. and Hong, C.S., 2006, February. Security in wireless sensor networks: issues and challenges. In Advanced Communication Technology, 2006. ICACT 2006. The 8th International Conference (Vol. 2, pp. 6-pp). IEEE.

[21] Madhav, K.V. and Selvaraj, R.L., 2010. A STUDY OF SECURITY CHALLENGES IN WIRELESS SENSOR NETWORKS. Journal of Theoretical & Applied Information Technology, 20(1).

[22] Singh, S. P., & Sharma, S. C. (2018). A PSO Based Improved Localization Algorithm for Wireless Sensor Network. Wireless Personal Communications, 98(1), 487-503.

[23] Misra, Sudip, Isaac Zhang, and Subhas Chandra Misra, eds. Guide to wireless sensor networks. Springer Science & Business Media, 2009.

[24] Raza, S., Duquennoy, S., Chung, T., Yazar, D., Voigt, T. and Roedig, U., 2011, June. Securing communication in 6LoWPAN with compressed IPsec. In Distributed Computing in Sensor Systems and Workshops (DCOSS), 2011 International Conference on (pp. 1-8). IEEE.

[25] Varadarajan, P. and Crosby, G., 2014, March. Implementing IPsec in wireless sensor networks. In New Technologies, Mobility and Security (NTMS), 2014 6th International Conference on (pp. 1-5). IEEE.

[26] Gandino, F., Montrucchio, B. and Rebaudengo, M., 2014. Key management for static wireless sensor networks with node adding. IEEE Transactions on Industrial Informatics, 10(2), pp.1133-1143.

[27] Sahingoz, O.K., 2013. Multi-level dynamic key management for scalable wireless sensor networks with UAV. In Ubiquitous Information Technologies and Applications (pp. 11-19). Springer, Dordrecht.

[28] Sahingoz, O.K., 2013. Large scale wireless sensor networks with multi-level dynamic key management scheme. Journal of Systems Architecture, 59(9), pp.801-807.

[29] Kuchipudi, R., Qyser, A.A.M. and Balaram, V.S., 2016, March. A dynamic key distribution in wireless sensor networks with reduced communication overhead. In Electrical, Electronics, and Optimization Techniques (ICEEOT), International Conference on (pp. 3651-3654). IEEE.

[30] Du, X., Xiao, Y., Guizani, M. and Chen, H.H., 2007. An effective key management scheme for heterogeneous sensor networks. Ad Hoc Networks, 5(1), pp.24-34.

[31] Mungara, R., VenkateswaraRao, K. and Pallamreddy, V., A Routing-Driven Elliptic Curve Cryptography Based Key Management Scheme for Heterogeneous Sensor Networks.

[32] Cui, B., Wang, Z., Zhao, B., Liang, X. and Ding, Y., 2015. Enhanced key management protocols for wireless sensor networks. Mobile Information Systems, 2015.

[33] Ahlawat, P. and Dave, M., 2018. An attack model based highly secure key management scheme for wireless sensor networks. Procedia Computer Science, 125, pp.201-207.

[34] Sun, D. and He, B., 2006. Review of key management mechanisms in wireless sensor networks. Acta Automatica Sinica, 32(6), p.900.

[35] Baek, S., Seo, S.H. and Kim, S., 2016. Preserving Patient's Anonymity for Mobile Healthcare System in IoT Environment. International Journal of Distributed Sensor Networks, 12(7), p.2171642.

[36] Nguyen-Vu, L., Park, J., Park, M. and Jung, S., 2016. Privacy enhancement using selective encryption scheme in data outsourcing. International Journal of Distributed Sensor Networks, 12(7), p.1550147716657255.

[37] Ban, H.J., Choi, J. and Kang, N., 2016. Fine-grained support of security services for resource constrained internet of things. International Journal of Distributed Sensor Networks, 12(5), p.7824686.

[38] Choi, S. and Kwak, J., 2016. Enhanced SDIoT security framework models. International Journal of Distributed Sensor Networks, 12(5), p.4807804.

[39] Eschenauer, L. and Gligor, V.D., 2002, November. A key-management scheme for distributed sensor networks. In Proceedings of the 9th ACM Conference on Computer and Communications Security (pp. 41-47). ACM.

[40] Alkhalaileh, M.N., Mestarihi, M. and Mohamad, I., 2014. Secure key management protocol for wireless sensor network.

[41] Hui, L. and Ying, C., 2010, November. A secure key management protocol for wireless sensor networks. In Education and Management Technology (ICEMT), 2010 International Conference on (pp. 660-662). IEEE.

[42] Seo, S.H., Won, J., Sultana, S. and Bertino, E., 2015. Effective key management in dynamic wireless sensor networks. IEEE Transactions on Information Forensics and Security, 10(2), pp.371-383.

[43] Vasala, U. and Sakthidharan, D.G., 2017. Effective Key Management In Dynamic Wireless Sensor Networks. International Journal of Computer Engineering in Research Trends, 4(7), pp.308-312.

[44] Goyal, P., Kumar, M. and Sharma, R., 2012. A Novel and Efficient dynamic Key Management Technique in Wireless Sensor Network. International Journal of Advanced Networking and Applications, 4(1), p.1462.

[45] Chen, C.L. and Li, C.T., 2008. Dynamic session-key generation for wireless sensor networks. EURASIP Journal on Wireless Communications and Networking, 2008(1), p.691571.

[46] Esposito, C., Ficco, M., Castiglione, A., Palmieri, F. and De Santis, A., 2018. Distributed Group Key Management for Event Notification Confidentiality among Sensors. IEEE Transactions on Dependable and Secure Computing.

[47] Suo, H., Wan, J., Huang, L. and Zou, C., 2012, March. Issues and challenges of wireless sensor networks localization in emerging applications. In Computer Science and Electronics Engineering (ICCSEE), 2012 International Conference on (Vol. 3, pp. 447-451). IEEE.

[48] Nirmala, A. P., & Paul, S. A. (2018). Security Challenges in Wireless Sensor Networks-A Review.

[49] Sarmad, U.K., Lavagno, L. and Pastrone, C., 2010, October. A key management scheme supporting node mobility in heterogeneous sensor networks. In Emerging Technologies (ICET), 2010 6th International Conference on (pp. 364-369). IEEE.

[50] Kumar, V., 2018. Improving Key Management Scheme Supporting Node Mobility in Heterogeneous Sensor Networks using Collision Keys.

[51] Zhang, Q., Yuan, J., Guo, G., Gan, Y. and Zhang, J., 2018. An Authentication Key Establish Protocol for WSNs Based on Combined Key. Wireless Personal Communications, 99(1), pp.95-110.

[52] Mall, D., Konaté, K. and Pathan, A.S.K., 2017, January. ECL-EKM: An enhanced Certificateless Effective Key Management protocol for dynamic WSN. In Networking, Systems and Security (NSysS), 2017 International Conference on (pp. 150-155). IEEE.

[53] Athmani, S., Bilami, A. and Boubiche, D.E., 2017. EDAK: An Efficient Dynamic Authentication and Key Management Mechanism for heterogeneous WSNs. Future Generation Computer Systems.

[54] Kamble, S.B. and Jog, V.V., 2017, May. Efficient key management for dynamic wireless sensor network. In Recent Trends in Electronics, Information & Communication Technology (RTEICT), 2017 2nd IEEE International Conference on (pp. 583-586). IEEE.

[55] Puthal, D., Nepal, S., Ranjan, R. and Chen, J., 2017. DLSeF: A dynamic key-length-based efficient real-time security verification model for big data stream. ACM Transactions on Embedded Computing Systems (TECS), 16(2), p.51.

[56] Kandah, F.I., Nichols, O. and Yang, L., 2017, January. Efficient key management for Big Data gathering in dynamic sensor networks. In Computing, Networking and Communications (ICNC), 2017 International Conference on (pp. 667-671). IEEE.

[57] Mahmood, Z., Ning, H. and Ghafoor, A., 2017. A Polynomial Subset-Based Efficient Multi-Party Key Management System for Lightweight Device Networks. Sensors, 17(4), p.670.

[58] Yagan, O. and Makowski, A.M., 2016. Wireless sensor networks under the random pairwise key predistribution scheme: Can resiliency be achieved with small key rings?. IEEE/ACM Transactions on Networking, 24(6), pp.3383-3396.

[59] Eschenauer, L. and Gligor, V.D., 2002, November. A key-management scheme for distributed sensor networks. In Proceedings of the 9th ACM Conference on Computer and Communications Security (pp. 41-47). ACM.

[60] Seo, S.H., Won, J., Sultana, S. and Bertino, E., 2015. Effective key management in dynamic wireless sensor networks. IEEE Transactions on Information Forensics and Security, 10(2), pp.371-383.

[61] Chan, H., Perrig, A. and Song, D., 2003, May. Random key predistribution schemes for sensor networks. In Security and Privacy, 2003. Proceedings. 2003 Symposium on (pp. 197-213). IEEE.

[62] Sarmad, U.K., Lavagno, L. and Pastrone, C., 2010, October. A key management scheme supporting node mobility in heterogeneous sensor networks. In Emerging Technologies (ICET), 2010 6th International Conference on (pp. 364-369). IEEE.

AUTHORS

Nesma Abd El-Mawla
Teaching Assitant at Communications and Electronics Dept. - Nile Higher Institute for Engineering and Science, Egypt

Mahmoud Badawy
Associate Professor at Computers and Systems Dept. - Faculty of engineering - Mansoura University, Egypt

Hesham Arafat
Full Professor at Computers and Systems Dept. - Faculty of engineering - Mansoura University, Egypt