Wireless Sensor Networks (WSNs): New trends in Secure Routing Techniques

Norhan Abdel-hamid
Computer Eng. and Control Sys Dept.
Faculty of Eng, Mansoura University, Egypt

Labib M. Labib
Computer Eng. and Control Sys Dept.
Faculty of Eng., Mansoura University, Egypt

Abdelhameed Ibrahim
Computer Eng. and Control Sys Dept.
Faculty of Eng., Mansoura University, Egypt

Hesham A. Ali
Computer Eng. and Control Sys Dept.
Faculty of Eng., Mansoura University, Egypt

ABSTRACT
Wireless Sensor Networks (WSNs), considered as one of the successfully distributed applications that are currently used to acquire knowledge and collect information from the wirelessly devices seamlessly. The distinctive architecture of WSNs contributed to deploy it in an extensive range of modern industrial applications such as surveillance, monitoring, predicted, and automated control systems which can help in bridging the divide between user requirements and technologies. Moreover, WSNs face several challenges such as Topology control, Robustness, Placement, Power consuming, Scalability, Reliability, Resource Utilization, QoS, Data availability and Security. The main objective of this paper can be classified into two parts; the first one is to illustrate WSNs architecture, applications, challenges, and recent research directions. The second one is highlighting on routing and security design issues, security threats, countermeasures against network layer attacks to achieve secure routing, as the efficiency of the communication process is mainly based on determining the best path between nodes. We also highlight the advantages and performance issues of each secure routing technique. At the end of this paper the possible future research areas are concluded.

Keywords
WSNs; automated control systems; routing; security; attacks.

1. INTRODUCTION
Wireless sensor networks (WSNs), is a type of wireless networks which are small, infrastructure less, and refer to a group of hundreds to thousands dedicated sensors. Those small sensors have limited power, and less expensive than any other traditional sensors. Those sensors are known as tiny devices that work together to collect data about the environment. After collecting data, sensors process and transmit the data to the base station, which supplies an interface between user and internet. The design of WSNs usually depends on the application, where many factors must be put into consideration such as cost, the environment, hardware, application's design objectives, and the constraints that will face the system [1, 2].
WSNs used in many applications [3,4], which reduce the gap between user requirements and technologies. From the most common applications in WSN is area monitoring, and military applications [5], at which sensors are used to detect enemy intrusion, environmental, earth tracking and monitoring. Monitoring has many sub-applications, some of those examples are: A) Air pollution monitoring that many cities deployed it to observe the concentration of the gasses that are dangerous. B) Forest fire detection in which sensor nodes are placed in the forest to detect when a fire has begun, and those nodes tooled up with sensors to measure humidity, temperature, and gasses produced by the fire. C) Water quality monitoring, by use of many wireless sensors it can create accurate maps for the status of water. D) Detection of the landslide that can be used to detect soil movement and the change in parameters of the soil. E) Natural disaster prevention which reduces the effect of environmental crisis such as floods. F) Healthcare monitoring applications that monitor patients and doctors in hospitals.
WSNs also used in industrial monitoring applications [3, 6] because sensors are infrastructure less and can be embedded into machines. WSNs could be utilized in many applications in this field such as machine health monitoring where sensors have been deployed in machine maintenance, water waste monitoring which can monitor water levels and the quality of underground and surface water, and structural health monitoring where WSNs can have control over civil infrastructure [7]. The sensor nodes consist of the radio transceiver, microcontroller, energy source, and external memory [8]. The radio transceiver connected to the internal or external antenna which transfers data and receives commands from the base station. The microcontroller is an electronic circuit which interfaces with the sensors, process, and stores the output of the sensors. The energy source that powers WSNs could be a battery, and it is very limited. The external memory is usually limited, and it depends on application requirements.
This paper aimed to represent the structure of WSNs, applications, and the anatomize challenges that face WSNs such as Topology control, Scalability, Robustness, Placement, Power consuming, Routing, security, and their recent research directions. Also, the paper represents a classification of routing protocols, and some routing techniques. Finally, the paper outlined many aspects that concern WSNs security: security requirements, various attacks types at the network layer in WSNs architecture, and it mentioned some new defense mechanisms against network layer attacks that help in achieving secure routing and give a further review to the interested researchers to complete with.
The rest of this paper is organized as the following: Section2 describes the WSNs basic and concepts. Section3 presents an overview of routing in WSNs its classification, challenges, and some of the routing techniques. Section 4 shows security in WSNs, its goals, network layer attacks, and their countermeasures. Section 5 presents in brief the future research directions, Finlay section 6 introduce the conclusion.

2. WSNS BASIC AND CONCEPT
In this paper the term sensor network is used to refer to a heterogeneous system join tiny sensors and actuators with

general purpose computing devices. It may consist of hundreds or thousands of low-power, low-cost nodes, perhaps mobile but more likely at fixed locations, deployed in masse to monitor and affect the environment. There are fundamental differences between any traditional wireless network and wireless sensor network [13]. Unlike traditional network WSNs have its design in which numbers of nodes are massive that may reach to millions depending on the application. Not only that but also nodes are less expensive than any traditional network. Moreover, WSNs has a processing ability (they contain microcontroller), sensing and communication ability. But traditional networks have no sensing ability. WSNs use broadcast communications while traditional networks use point-to-point communications. Moreover, WSNs are event-driven or environment-driven, when any event happens, or any changes in the environment occur, sensor networks collect data or generate it. While in traditional networks, human creates data, so the pattern of the traffic changes from time to time. Sensor nodes density is high and has limited resources like memory and processing, while in contrary, traditional network node density is low, and its memory size is large. When it comes to energy, WSNs consume less energy than any traditional network, and it is easy to expand or reduce the coverage area.

WSNs are divided into two sectors: structured and unstructured WSNs [8]. The Unstructured WSNs consists of a massive number of tiny randomly deployed nodes in the area, the network in the unstructured WSN is unattended to perform reporting and monitoring functions, and it is hard to perform network maintenance as detecting a failure and managing connectivity. On the other hand, in structured WSNs all sensors are placed in a pre-planned technique where nodes are placed at fixed places which help in providing full coverage, the network maintenance and management cost is low.

Not like wired networks [13], routing in WSNs faces various types of challenges as a reason of the distinctive characteristic of sensor nodes [19]. WSNs may be exposed to failure due to the hard deployment environments [9]. Sensor nodes should be independent in the network area [10] , this self-independent allows all nodes to interact with each other through wireless basis, which leads to topology changes. As a result, different attacks give a chance for many security problems [20]. For example, the attacker could have the opportunity to fake the sensor node, spy on data transmission, proceeds false messages, and waste network recourses. Therefore, providing security to such network is essential to route data from its source to its final destination [38]. Putting all those into consideration, there are many limitations in combining security into a wireless sensor network [34]. Those limitations could be in energy [18], computation, processing, memory, and communication capabilities [11]. As a result, to create a secure protocol, those limitations have to be put in consideration. Not only that but reaching acceptable performance levels to satisfy the needs of a specific application is also a desired goal. Whereas, security counts an important factor in data communications [12].

In reality, the WSNs applications are fairly numerous. As, WSNs have profound belongings on military and public applications such as target field imaging, weather monitoring, intrusion detection, security and tactical surveillance, detecting ambient conditions such as temperature, movement, sound, light, or the attendance of certain objects, and disaster management. Deployment of a sensor network in such applications can be in random fashion or manual. Designing a network of these sensors can aid rescue operations by locating survivors, identifying risky areas, and making the rescue team more aware of the overall situation in a disaster area.

3. RECENT RESEARCH DIRECTIONS

WSN receives significant attention, but it faces a lot of constraints and challenges such as Topology control, Scalability, Robustness, Placement, Power consuming, Routing, Security, and Data availability. Table 1 concludes the most important research directions of WSN challenges in brief.

4. ROUTING ISSUES

Routing is process to find the best path to deliver the data from the source sensor node to the destination sensor node. It is vital in WSN than any other networks due to many characteristics as an IP-based schema which is routing protocols in which the traffic is routed from nodes to the base station. In WSNs, nodes are resource constrained regarding energy [22], storage, and Computational capacity, so it must be used efficiently. Routing protocols that are organized into three categories: the first one is based on a mode of functioning which is classified into proactive, reactive and hybrid routing [23]. The second one relies on participation style of nodes which are classified into flat, direct, and clustering routing protocols [24]. Moreover, the third one based on the network structure divided into Hierarchical [25], Data Centric [26], and Location-Based [27]. Many factors affect routing protocols that must be taken in consider when designing routing protocols [28, 29]. Some of these factors are Node Deployment, Fault-Tolerance, Scalability, Data Aggregation, Routing Looping Problem, Energy Constraints, and Security which consider from the most important factor to achieve secure routing.

4.1 Routing techniques

In this section, we discuss some routing techniques, showing their characteristics, type, advantage, and disadvantage. As shown in Table 2

Table1: Recent research directions for WSN

Challenges	Approaches	Objectives	Future directions
Topology control	A new distributed topology control algorithm, called the Cooperative Topology Control with Adaptation (CTCA) [14]	Change transmission power of nodes to increase based on a game-theoretic approach that maps the problem of maximizing the network's lifetime into an ordinal potential game network lifetime	Improve the method to be more generalized
	A new link interference model [56]	Measures the interference of a link by counting the number of links that are covered in order to reduce link interferences	Designing efficient distributed algorithms to construct interference-optimal topologies

	Cooperative Topology Control with Adaptation (CTCA) [57]	Change nodes transmission powers to extend the network lifetime	Developing and describing a generalized version of this approach
Scalability	A reduced scale-free network mode based on the traditional theory of scale-free network [15]	Balance the energy costs across the entire network and enhance the robustness	Improving the model with the presence of epidemic threshold to avoid an unpredicted result.
	Multi-hop routing (HYMN) [58]	Improve the Scalability of Wireless Sensor Networks.	Developing this approach to be more efficient
Robustness	Gene Regulatory Networks (GRNs) [16]	Face maximize efficiency problem in which sensor nodes should be vigorous and flexible to any failures	Improve the algorithm to be more efficient
	A novel solution to obtain robust WSNs [59]	Improving the robustness of communications in WSNs by exploiting principles of biological robustness at Nano scale	Evaluate the application of GRNs to other network scenarios, such as the Internet.
Placement	New relay placement approach [17]	Have the ability to increase the connectivity of the network in wireless multi- hop network.	Purpose a new intelligent routing protocol which uses 2-relay nodes connected.
	Sink Node Placement Strategies for WSNs [60]	Find the optimal position from a perspective of the network lifetime in the single-hop WSNs and multi-hop WSNs	Improve the strategy to increase network lifetime
	Weighted relay node placement for WSN connectivity [61]	Minimize the total weight of the points on which the relay nodes are deployed	Study weighted relay node placement problem for robust and survivable WSN
Power consuming	Topology control algorithm called A tree based heuristic [18]	Increase the lifetime of the network via decreasing energy consumption of the network by switching off some of the active nodes at random by keeping the connectivity of the whole network	Improve the algorithm by using small global information
	An energy efficient, mobile sink based data collection protocol for large scale WSNs [62]	This algorithm deal with frame loss caused by multipath fading, improving frame delivery rate while suppressing energy consumption and data collection time	Refine the proposed method to reduce data collection time by using parallel transmissions, and extend this proposed method to cope with node failure
Routing	A polynomial time heuristic algorithm [19]	The performance of the network can be improved by taking into consideration the dynamic channel assignment while routing can make more transmissions, It can also efficiently decrease the computational complexity and solve the linear programming formulations	Reduce equations to decrease computational time to improve network performance
	Energy Efficient and Trustable Routing Protocol for wireless sensor networks based on genetic algorithm (E2TRP) [63]	Dynamic formation of CH and clusters based on distance of the nodes from CH (of the sensor nodes) using genetic algorithm and trust of the sensor nodes	Developing and describing a generalized version of this approach
	Improved clustering algorithm based on energy consumption in wireless sensor networks [64]	Protect the nodes with low energy and long distance for preventing the failure of the energy to be the cluster-heads.	How to deal with the initial energy when it is not at the same time
Security	New mechanisms that based on data-gathering for a large sensor network area when using one M-investors or more [20]	Supply security for both inputted data memory and outside network message.	Improving mechanism to increase the security over an enormous wide area.
	Position Responsive Routing Protocol (PRRP) [65]	Improving the network lifetime by reducing the energy consumption of each sensor node	Improve the protocol to deal with mobile ad-hoc network

Table2: Routing protocols summary

Approaches	Protocols	Characteristics	Advantage / Disadvantage
Re-active Routing Technique	Ad-hoc On-Demand Distance Vector (AODV) [30]	Is an incorporation of on-demand and distance-vector, not only that but a method of routing a message, whereby message could be passed by exploring routes	Advantages Flat routing protocol where there is no need to the central administrative system that handles routing process, avoid loops and counting to infinity problem. It keeps small message overhead. The connection setup delay is lower. It establishes the shortest path with lowest power consumption. It is used in solving black hole problem.
			Disadvantage • Takes much time to build the routing table. • Consumes more share bandwidth. • Higher processing demand
	Dynamic Source Routing (DSR) [31]	An On-Demand routing protocol, in which it calculate route only when it is necessary. Node discovers the route by sending the route request to all neighbors that contain unique id, the list of nodes, source address, and destination address.	Advantage • It uses no periodic routing. It reduces bandwidth overhead. • Protect battery power. • Reduce route maintenance overhead. • The route is caching also decrease the overhead gained from route discovery.
			Disadvantage • Packet header become larger with route length • The problem of Route replay storm.
Pro-Active Routing Technique	Destination-Sequenced Distance-Vector (DSDV) [32]	Is table-driven algorithm which depends on Bellman-ford algorithm [39], where every node maintain a routing table arranged in sequence that verifies next hop, cost and the cost metric of each destination	Advantage • The simple routing protocol that is designed for initiating ad-hoc network with fewer sensor nodes. • It does not include format loops because it uses destination sequence numbers • No latency caused by route discovery.
			Disadvantage • There are bandwidth and power consumed by sleeping nodes even if the network is idle • Most route information never used. • Not the right choice for highly dynamic network
Hierarchical Routing Technique	Low-Energy Adaptive Clustering Hierarchy (LEACH) [33]	Works on dividing data into clusters to decrease the consumption of energy. This operation consists of several rounds divided into two phases: Step up phase, and steady phase.	Advantage • It gives the sensor node a longer lifetime. • It reduce network traffic as it aggregates all data at the cluster head • It does not need location information of nodes to create cluster • It saves energy.
			Disadvantage • It does not give information about cluster head in the network. • Clusters are randomly divided which causes uneven distribution of the clusters which lead to increase power consumption. • It is not suitable for application with extensive place coverage.

4.2 Security Issues

Security is the critical issue especially in WSNs for many reasons; some of these reasons are that all wireless nodes are usually found in the hazardous environment and the broadcast nature of WSN which make it easy to be effected from any attack. There are many security goals must be achieved, these security goals [34, 35, 36] can be classified to primary goals, and secondary goals. The primary goals which are called standard security goals such as: data confidentiality, data authentication, data integrity, and data availability. The secondary goals [37] like data freshness, self-organization, time synchronization, and secure localization.

4.3 Threats to Routing Protocols

In this section we now explore vulnerabilities and possible attacks. Broadly speaking, there are two kinds of attacks. One is the active attack, which is an attempt to improperly modify data, gain authentication, or gain authorization by inserting false packets into the data stream or by modifying packets transiting within the data stream. Second is the passive attack, which is an attack on the authorization system which inserts nothing into the data stream, but instead passively monitors information being sent between other parties. For attacks to routing protocols, our main concern is active attack.

4.3.1 Requirements for Secure Routing Protocols

Despite the various types of attacks, they in fact take the chance of the Shortage of authenticity, availability, integrity. We now set those services in the condition of secure routing protocols.

1. Data Authentication: it explains the senders and the receivers' identity so that the receiver makes sure that arrived data was delivered by the claimed sender [36]. Adversary not only can modify the packet data, but also replace the packet stream by adding additional false packets, so the destination have to make sure that the used data is received from the right source.
2. Data Availability: to ensure that the data needed is available all the time even if any failure happens [66]. It is important to preserve network operation so nodes are capable of using the resources, or whether the network is ready for communication at any time. Thus availability is a primary important for maintain a network.
3. Data Integrity: it has to confirm that the message is well received where data is not changed, or tempered with [66], and to make sure that the data is reliable. The unstable condition or the existence of any malicious nodes may lead to a serious damage, or waste of data, which may cause the system to lose its integrity.

In general, to secure routing protocols it first requires analyzing the protocol to determine its vulnerabilities and possible threats. Second, determining security requirements based on the existing environment. Finally, authentication mechanisms and cryptographic techniques should be integrated into the design to address these issues.

4.3.2 Mechanisms for Secure Routing Protocols

Generally, in terms of intended use, accessibility, and network connectivity, different security mechanisms may be needed to address the security requirements [67]. Cryptography is security mechanisms used to help secure routing protocols, it is the basis for secure anything. Cryptography can supply integrity and confidentiality of data or information of traffic flow. It can be used either alone or with some other security mechanisms. A cryptographic algorithm should be reversible and there are two common classifications of reversible encryption algorithms: symmetric cryptographic algorithms which are known as secret key, where the encryption key knowledge refers to the knowledge of the decryption key and vice-versa. And symmetric encryption algorithms which are known as public key, where the encryption key knowledge does not refers to the knowledge of the decryption key or vice-versa. There also another type of cryptographic algorithm which in known by message digests function.

4.3.3 Network Layer Attacks and Countermeasure

In previous sections, two important issues which are routing and security issues are discussed. In this section, some network layer attacks are represented [38] and their defense mechanisms to achieve secure routing as shown in Table 3.

5. FUTURE RESEARCH DIRECTIONS

Although there is various works done on WSN security, there are a lot of open issues that need to be solved. Presently WSNs security research is completed in a fragmented manner in which every group focuses on fixed problems or aspects. There are various areas that concern with secure routing must be investigated as there must be faster coverage because the gauge of WSNs operation is enormous which have thousand or million sensor nodes, WSNs have dynamic topology, and routing tables also subject to prompt changes so the routing protocols must be fast coverage. There must also be energy optimized routing protocols that help in enhancing the efficiency while providing security against the various attacks that network face. As shown in Fig 1: future directions of research on routing protocols in WSNs. The future directions of research on routing protocols in WSNs have to concentrate on the following:

1. Realizing nodes mobility and multi-sink with accomplishing security and requirements of QoS to the new routing protocols. Those new protocols will assist in protecting networks and extend their life time.
2. Many learning algorithms depend on using partial data and feedback, in which the discovery methods of the route update to book all convenient routes from source to reach the desire destination, and through the different route, the packets are divided and communicated. Feedback is gained to evaluate paths performance which makes dynamic data allocation assure maximum efficiency. It is evident that such a scheme will encourage proper routing randomness. Furthermore, the data is divided arbitrarily into various routes. Those factors supply superb inviolability versus different types of attacks.

Table 3: Network layers attacks and their countermeasures

Attack Types	Sybil attack	Hello flood attack	Selective forwarding attack	Sinkhole attack	Wormhole attack
Attack definition	A malignant node appears to be set of nodes either by fabrication or stealing the identities of valid sensor nodes [39]. Malignant nodes send to nodes in the network invalid data to mislead them. Attackers seem as they are located in several locations at the same time. This attack is extremely dangerous to protocols of geographic routing.	Sending HELLO packets to all network nodes in which the attackers send high power packet to cheat all neighbors and make them feel one of their neighbors. All nodes respond the HELLO message and waste their energy. Not only the use of authenticated broadcast protocols help in preventing HELLO flood attacks, but also verifying bi-directionality of local prevent those attacks.	It occurs when there is a malignant node in the network that acts as the black hole. Malicious nodes decline to send any packets and drop them.	The attacker creates a compromised node which is located in the middle of several areas. This node attracts the near data from a particular area that destined to the base station. [39]. This hole is almost near to the BS to make malicious node act as a BS [55].	Repetition of messages from different locations via low latency links. Wormhole nodes work fully unseen [55]. This type of attack considers from the most dangerous attack in wireless sensor network. It may also be done in the initial stage when sensors begin to explore neighbor's data.
Attack result	The result of the attack may be complete degeneration of network service. Shattering data integrity. The disruption of multi-path and geographic routing protocols. Corruption of packets. Routing information modification. Wrong sensor reading.	Disrupting topology construction. Destruction of the Network and routing. Overwrought nodes energy. Decrease the efficiency. Increase latency of WSNs. Loss of packets.	Modifying or dropping messages. Have an Impact on WSNs traffic. Verifying malicious nodes is impossible.	Originate a huge "sphere of influence" in sensor networks. Routing information fabrication and modification. Dropping of packets. All network resource exhaustion. Make other attacks as eavesdropping.	Misdirection of routes. Change of network topology. Routing perturbation. False routing information. WSN disruption. Changing stream of the messages.
Security class	Fabrication, modification	Fabrication, interruption	Modification	Fabrication, modification	Interception, Fabrication
Attack threat	Integrity, availability, authenticity	Authenticity, availability	Integrity, availability	Authenticity, availability, integrity	Authenticity, Confidentiality
Attacker location	Internal	Internal	Internal	Internal	External
Defense mechanisms	CAM-PVM METHOD [40] RADS technique [41]	BAP Technique [42] CHMD Algorithm [43] Location Verification Scheme[44] Energy Level Based Scheme[45]	PACK based schema [46] Multipath routing scheme [47] SCHEMAS schema [48]	Optimized AODV Routing [49] [50] Optimal Cluster Head Selection Based Energy Efficient Technique[51] A Novel Agent-Based Approach[52]	Using (AODMV) protocol [53] Range-Free Localization [54]

3. Most conventional schemes that concern on routing are layout to communicate using optimal paths. It is visible that WSNs are rested on a resource, such a scheme quickly bring down the resources over the optimal paths. Moreover, it can make the system more predictable. It is the related note to that all packets are sent via a single path which makes routing protocols more fragility to any attacks. The energy-aware algorithm is enhanced to gauge these problems.

4. There are many protocols that help in solving WSNs security threats, but until now there is no common protocol or technique that can solve all security threats and satisfy all requirement domains. As in [41], the authors represent a rule-based anomaly detection system called RADS that can observe and detect timely Sybil attacks in wide range WSNs. This protocol does not need any cryptography methods or third trusted party authorities; it minimizes the overhead caused by sensor nodes communication, it consider as cost-effective where each node could detect more than one Sybil attack without the need of any additional hardware enforcement. However, this system cannot support the detection of indirect Sybil attacks. The author should expand the system capabilities to detect more threats like the worm hole, hello flood, and sinkhole attacks. The author also should use stochastic environment and real attack patterns to make the system support in direct Sybil attacks. Finally, they have to make RADS method prevent power consumption as it considers the very critical issue to WSNs. We are going to develop RADS procedure to detect more threats types not only Sybil attacks, with putting power consumption in consideration.

Finally, our future direction is to develop an algorithm which has the ability detect and face more than on threat type like worm hole, hello flood, Selective forwarding, and sinkhole attacks, with putting energy consumption in consideration as it considers very critical issue to WSNs, and to ensure correct packets delivery with reduced energy consumption

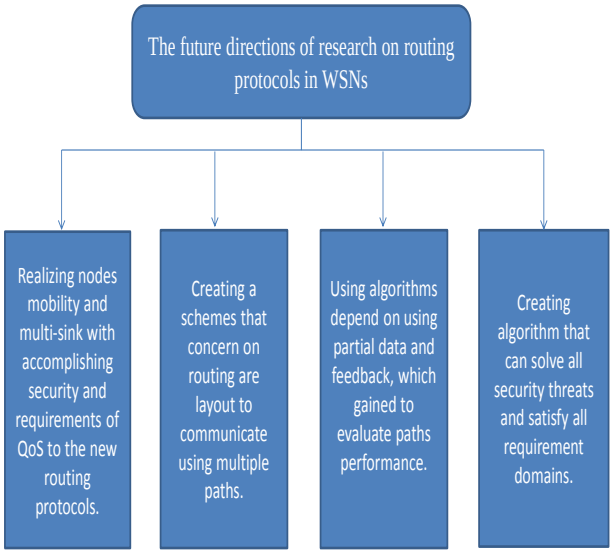

Fig 1: Future Research directions

6. CONCLUSION

The significance of WSNs cannot be negation because the computing world becomes compact and portable. WSNs face various security challenges because of their wireless common medium, heterogeneous tough recourses, and unpredictable topology. While routing in WSNs is a process to find the best path among nodes, but data in this route expose to different types of attacks such as Sybil, Hello Flood, Wormhole, Sinkhole, and Selective forwarding attacks. In which the adversary concern with injecting the network with false data or sabotage it. So it is necessary to create effective defense mechanism against those attacks. However, designing a sensor network routing protocol which offset both security goals and fulfills energy savings of state-of-art of sensor routing protocols is still an open area. That is because such protocols depend on self-regulation, nodes, and BS which contain local information only. Moreover, to achieve security the system should be globally known, and this task is too expensive for sensor networks. Also, security is multi-layered issues in which if data is injected in any layer, it cannot transmit to the next layers, so multi-security solutions which provide a full security extend to all entire protocol stacks are needed.

6. REFERENCES

[1] Jennifer Yick, Biswanath Mukherjee, DipakGhosal, 2008, Wireless sensor network survey, Computer Networks 52, 2292-2330.

[2] ShabbirHasan, Md. ZairHussain, R. K. Singh, 2013, A Survey of Wireless Sensor Network," International Journal of Emerging Technology and Advanced Engineering 3, (Mar. 2013), 487-492.

[3] Daniele Puccinelli, Martin Haenggi, 2005, Applications and Challenges of Ubiquitous Sensing, IEEE Circuits and system magazine, 19-29.

[4] MohdFauziOthmana, KhairunnisaShazalib, 2012, Wireless Sensor Network Applications: A Study in Environment Monitoring System. In Procedia Engineering, International Symposium on Robotics and Intelligent Sensors 41, 1204-1210

[5] S.Prasanna, SrinivasaRao, 2012, An Overview of Wireless Sensor Networks Applications and Security. International Journal of Soft Computing and Engineering (IJSCE) , (May 2012), 538-540

[6] HimaniChawla, 2014, Some issues and challenges of Wireless Sensor Networks. International Journal of Advanced Research in Computer Science and Software Engineering 4, (July 2014), 236-239

[7] Shiva Mirshahi, AliakbarAkbari, SenerUysal, " Implementation of Structural Health Monitoring based on RFID and WSN," Proceeding of the IEEE 28th Canadian Conference on Electrical and Computer Engineering Halifax, Canada, May 2015, pages 1318-1323

[8] Siddhi Sharma FET, India Deepak Sethi FET, India P. P. Bhattacharya, 2015, Wireless Sensor Network Structural Design and Protocols: A Survey. Foundation of Computer Science FCS, New York, USA, (June 2015), 32-36.

[9] Jing Chen, Ruiying Du, Qian Wang, ShixiongYao, 2013, Secure Routing Based on Network Coding in Wireless Sensor Networks. 12th IEEE International Conference on Trust, Security and Privacy in Computing and Communications, 58-64.

[10] Kai Lin · Chin-Feng Lai · Xingang Liu · Xin Guan, 2012, Energy Efficiency Routing with Node Compromised Resistance in Wireless Sensor Networks. Mobile NetwAppl, , 75-89.

[11] M. Brandl, KH Kellner, T. Posnicek, A. Kos, C. Mayerhofer, C. Fabian, 2009, An Efficient Source initiated On-Demand Data forwarding scheme for Wireless Sensor Networks. In proceedings of the 7th International Conference on information communications and Signal Processing (ICICS), 1-7

[12] AbrorAbduvaliyev, Al-Sakib Khan Pathan, Jianying Zhou, Rodrigo Roman, and Wai-Choong Wong, 2013, On the Vital Areas of Intrusion Detection Systems in Wireless Sensor Networks, IEEE COMMUNICATIONS SURVEYS & TUTORIALS 15, 1223-1237

[13] KiranMaraiya, Kamal Kant, Nitin Gupta, 2011, Application based Study on Wireless Sensor Network, International Journal of Computer Applications 21, (May 2011), 9-15

[14]Xiaoyu Chu and Harish Sethu, 2015,Cooperative Topology Control with Adaptation for improved lifetime in wireless sensor networks. Ad Hoc Networks 30, (July 2015), 99-114

[15] Neha Keshri, Anurag Gupta, Bimal Kumar Mishra, 2016, Impact of reduced scale free network on wireless sensor network. Physica A: Statistical Mechanics and its Applications 463, (December 2016), 236-245.

[16]Azade Nazi1, Mayank Raj, Mario Di Francesco,PreetamGhosh, Sajal K. Das, 2014, Robust Deployment of Wireless Sensor Networks Using Gene Regulatory Networks. Pervasive and Mobile Computing 13, (August 2014), 246-257

[17] Roberto Magán-Carrión, RafaelA. Rodríguez-Gómez, JoséCamacho, Pedro García-Teodoro,2016, Optimal relay placement in multi-hop wireless networks. Ad Hoc Networks 46, (August 2016), 23-36.

[18] Hui Wang H. Eduardo Roman, Liyong Yuan, Yongfeng Huang, Rongli Wang, 2014, Connectivity, coverage and power consumption in large –scale wireless sensor network. Computer networks 75, (24 December 2014), 212-225.

[19] Jinbao Li a, XiaohangGuo, LongjiangGuo, ShoulingJi b, Meng Han, ZhipengCai, 2015, Optimal routing with scheduling and channel assignment in multi-power multi-radio wireless sensor networks. Ad Hoc Networks, 45-62

[20] S.SangeethaMariammala, J.Gayathrib,2015, Ensuring higher security for gathering and economically distributing the data in social wireless sensor networks. Procedia Computer Science 47, 408-416.

[21] Sergio F. Ochoa, Rodrigo Santos, 2015, Human-centric wireless sensor networks to improve information availability during urban search and rescue activities. Information Fusion 22, (March 2015), 71-84.

[22] Mostefa BENDJIMA, Mohamed Feham, 2015. Multi-Agent System for a Reliable Routing in WSN. Science and Information Conference London, UK, (July 2015), 1412-1419

[23] FALEH Rabeb, NASRI Nejah, KACHOURI Abdennaceur, SAMET Mounir, 2012. An Extensive Comparison of DSDV, DSR and AODV Protocols in wireless sensor network. International Conference on Education and e-Learning Innovations.

[24] Santar pal singh, s.c.sharma, 2015, A Survey on Cluster Based Routing Protocols in Wireless Sensor Networks. Procedia Computer Science, International Conference on Advanced Computing and Applications 45, 687-695.

[25] ZahariahManap, BorhanuddinMohd Ali, CheeKyun Ng, Nor KamariahNoordin, AduwatiSali, 2013, A Review on Hierarchical Routing Protocols for Wireless Sensor Networks. Wireless Personal Communications 72, (September 2013), 1077-1104

[26] A.G.Gokula Kumar, R.Thiyagarajan, N.Sripriya, 2014, Data Centric Based Routing Protocols for Wireless Sensor Networks: A Survey, International Journal of Scientific and Research Publications 4, (December 2014), 2250-3153.

[27] Aditya H. Iche, Dhage, 2015, Location based Routing Protocols: A Survey, International Journal of Computer Applications 109, (January 2015), 28-31.

[28]Rajashree.V.Biradar, V.C.Patil, S.R.Sawant, Dr.R.R.Mudholkar, Classification and comparison of routing protocols in Wireless Sensor Networks. UbiccJournal, 4, 704-711

[29] Khushboo Gupta, VaishaliSikka, 2015, Design Issues and Challenges in Wireless Sensor Networks. International Journal of Computer Applications 112, (February 2015), 26-32

[30] P.Samundiswary and P.Dananjayan, 2010, Performance Analysis of Trust Based AODV for Wireless Sensor Networks. International Journal of Computer Applications 4, (August 2010), 6-13.

[31] Parul Kansa, DeepaliKansal, ArunBalodi, 2010, Comparison of Various Routing Protocol in Wireless Sensor Network. International Journal of Computer Applications 5, (August 2010), 14-19.

[32] I.F.Akyildiz, S.W.Sankarasubramaniam, E.Cayirci, 2002, A survey on sensor networks. IEEE Journal of Communication 40, 102-114.

[33] Rajendra Prasad Mahapatra, Rakesh Kumar Yadav, 2015, Descendant of LEACH Based Routing Protocols in Wireless Sensor Networks. Procedia Computer Science 57, 2015, 1005-1014

[34] G. Bianchi, 2010, A comparative study of the various security approaches used in wireless sensor networks. International Journal of advanced science and technology 17, (April 2010) , 31-44.

[35] Idrees S. Kocher, Chee-Onn Chow, Hiroshi Ishii, Tanveer A. Zia, Threat Models and Security Issues in Wireless Sensor Networks, International Journal of Computer Theory and Engineering 5, (October 2013), 830-835

[36] MahsaTeymourzadeh, RoshanakVahed, SoulmazAlibeygi, NargesDastanpor, 2013, Security in Wireless Sensor Networks: Issues and Challenges. International Journal of Computer Networks and Communications Security 1, (December 2013) , 329-334

[37] MahfuzulhoqChowdhury, MdFazlulKadera, Asaduzzaman, 2013, Security Issues in Wireless Sensor Networks: A Survey. International Journal of Future Generation Communication and Networking 6, 97-116.

[38] Harsh Kumar Verma, Saurabh Singh, 2011, Security for Wireless Sensor Network. International Journal of Computer Science and Engineering (IJCSE), (June 2011), 2393-2399.

[39] S.Mohammadi, R.A.Ebrahimi and H.Jadidoleslamy, 2011, A Comparison of Routing Attacks on Wireless Sensor Networks. International Journal of Information Assurance and Security (JIAS) 6, 195-215.

[40] MANJU V C, 2014, Sybil attack Preventation in Wireless Sensor Network. International Journal of Computer Networking, Wireless and Mobile Communications (IJCNWMC) 4, (Apr 2014), 125-132.

[41] PanagiotisSarigiannidis, EiriniKarapistoli, Anastasios A. Economides, 2015, Detecting Sybil attacks in wireless sensor networks using UWB ranging-based information. Expert Systems with Applications, 7560-7572

[42] Gayatri Devi1, RajeebSankar Bal2, Nibedita Sahoo3, 2015, Hello Flood Attack Using BAP in Wireless Sensor Network. International Journal of Advanced Engineering Research and Science (IJAERS) 2, (January 2015), 80-86.

[43] YayaShen, SanyangLiu,Zhaohui Zhang, 2015, Detection of Hello Flood Attack Caused by Malicious Cluster Heads on LEACH Protocol. International Journal of Advancements in Computing Technology (IJACT) 7, (March 2015), 40-47

[44] Rawan S. Hassoubah, Suhare M. Solaiman, Manal A. Abdullah, 2015, Intrusion Detection of Hello Flood Attack in WSNs Using Location Verification Scheme. International Journal of Computer and Communication Engineering 4, (May 2015), 156- 165

[45] DilpreetKaur, Rupinderpal Singh, 2015, "Energy level based Hello Flood Attack Mitigation on WSN," International Journal of Embedded Systems and Computer Engineering, (July 2015), 1551-1554.

[46] Anfeng Liu, Mianxiong Dong, Kaoru Ota and Jun Long, 2015, PHACK: An Efficient Scheme for Selective Forwarding Attack Detection in WSNs. Sensors, 30942-30963.

[47] Geethu P C, Rameez Mohammed A, 2013, Defense Mechanism against Selective Forwarding Attack in Wireless Sensor Networks. IEEE – 31661, 4th ICCCNT, (July 2013), 1-4.

[48] Ji Won Kim, Soo Young Moon, Tae Ho Cho, JinMyoung Kim, Seung Min Park, 2011, Improved message communication scheme in selective forwarding attack detection method. Digital Content, Multimedia Technology and its Applications (IDCTA), 7th International Conference, 2011

[49] AnandMotwani, VimalDhote, 2016, Optimized AODV Routing for Effective Attack Security in Wireless Sensor Networks. International Journal of Electrical, Electronics, and Computer Engineering, 33-40.

[50]Vandana B. Salve, Leena Ragha,NileshMarathe, 2015, AODV Based Secure Routing Algorithm against Sinkhole Attack in Wirelesses Sensor Networks. IEEE International Conference on Electrical, Computer and Communication Technologies (ICECCT), 1-7.

[51] Snehal P. Dongare, Prof. R. S. Mangrulkar, 2016, Optimal Cluster Head Selection Based Energy Efficient Technique for Defending against Gray Hole and Black Hole Attacks in Wireless Sensor Networks. International Conference on Information Security &Privacy, 11-12 December 2015, Nagpur, INDIA, Procedia Computer Science, 423-430.

[52] SinaHamedheidari, Reza Rafeh, 2013, A Novel Agent-Based Approach to Detect Sinkhole Attacks in Wireless Sensor Networks. Computers & Security, 1-14.

[53] ParmarAmisha, V.B.Vaghela, 2016, Detection and Prevention of Wormhole Attack in Wireless Sensor Network using AOMDV protocol. Procedia Computer Science Published by Elsevier, 7th International Conference on Communication, Computing and Virtualization, 700-707.

[54] Mariano García-Otero, AdriánPoblación-Hernández, 2012, Detection of Wormhole Attacks in Wireless Sensor Networks Using Range-Free Localization. IEEE 17th International Workshop on Computer Aided Modeling and Design of Communication Links and Networks (CAMAD), 21-25

[55] JunaidAhsenaliChaudhry, Usman Tariq, Mohammed Arif Amin, Robert G. Rittenhouse,2013, Dealing with Sinkhole Attacks in Wireless Sensor Networks," Advanced Science and Technology Letters 29, 7-12.

[56]Guodong Sun, LinZhao, ZhiboChen, GuofuQiao, 2015, Effective link interference model in topology control of wireless Ad hoc and sensor networks. Journal of Network and Computer Applications 52, 69-78

[57]Xiaoyu Chu, Harish Sethu, 2015, Cooperative Topology Control with Adaptation for improved lifetime in wireless sensor networks. Ad Hoc Networks 30, 99-114

[58]Ahmed E.A.A. Abdulla, Hiroki Nishiyama, Nirwan Ansari, Nei Kato, 2011, HYMN to Improve the Scalability of Wireless Sensor Networks. The Third International Workshop on Wireless Sensor, Actuator and Robot Networks, 519-524.

[59]Azade Nazi, Mayank Raj, Mario Di Francesco, PreetamGhosh, and Sajal K. Das, 2016, Efficient communications in Wireless Sensor Networks Based on Biological Robustness. International Conference on Distributed Computing in Sensor Systems, 2016, 161-168.

[60]Fengchao Chen, Ronglin Li, 2013, Sink Node Placement Strategies for Wireless Sensor Networks. Wireless PersCommun, 303-319.

[61] SenerKimence, IlkerBekmezci, 2013, Weighted relay node placement for wireless sensor network connectivity. Wireless Netw, 624-627.

[62]Masanari Iwata, Suhua Tang, SadaoObana, 2017, Sink-Based Centralized Transmission Scheduling by using Asymmetric Communication and Wake-up Radio. Wireless Communications and Networking Conference (WCNC), IEEE.

[63] Soumitra Das, Dr. Barani S, Dr. SanjeevWagh, Dr.S.S.Sonavane, 2016, Energy Efficient and Trustable Routing Protocol for wireless sensor networks based on genetic algorithm (E2TRP). International Conference on

Automatic Control and Dynamic Optimization Techniques (ICACDOT), 154-159.

[64] Wenliang Wu, NaixueXiong, Chunxue Wu, 2017, Improved clustering algorithm based on energy consumption **in wireless** sensor networks. IET Networks, The Institution of Engineering and Technology, 1-7.

[65] Noor Zaman, Low Tang Jung, Muhammad MehboobYasin, 2016, Enhancing Energy Efficiency of Wireless Sensor Network through the Design of Energy Efficient Routing Protocol. Journal of Sensors, 1-16.

[66] Rujkumar, 2012, A Survey on Security Attacks in Wireless Sensor Network. "International Journal of Engineering Research and Applications (IJERA) 2, (July-August 2012), 1684-1691.

[67] Feiyi Wang, Brian Vetter, Shyhtsun Felix Wu, 1997, Secure Routing Protocols: Theory and Practice. U.S. Department of Defense Advanced Research Projects Agency and the U.S. Air Force Rome Laboratory, 1-14.