Secure Routing in Wireless Sensor Networks: A State of the Art

A. M. Riad
Dean of Faculty of Computers and Information Sciences, Mansoura University, EGYPT

Hamdy K. El-Minir
National Research Institute of Astronomy and Geophysics, Helwan, EGYPT

Mohamed El-hoseny
Ass. Lecturer at Faculty of Computers and Information Sciences, Mansoura University, EGYPT

ABSTRACT.
Wireless Sensor Networks (WSNs) have attracted intensive interest from both academia and industry due to their wide application in civil and military scenarios. Recently, there is a great interest related to routing process in WSNs. Security aspects in routing protocols have not been given enough attention, since most of the routing protocols in WSNs have not been designed with security requirements in mind. This paper surveys the current challenges of WSN. It will focus on the attempts of building an Artificial Intelligence (AI) based routing protocols in WSNs. This paper also identifies the WSN security trends and threats. The paper also addresses some examples of how to use artificial intelligence in the routing algorithms and shows the advantages and the drawbacks of each. A proposed framework also has been introduced. Finally, the future directions of WSNs have been declared.

Keywords
Wireless Sensor Network, Routing Protocol, Artificial Intelligent,

1. INTRODUCTION
We ask that authors follow some simple guidelines. In essence, we ask you to make your paper look exactly like this document. The easiest way to do this is simply to download the template, and replace the content with your own material.

Wireless sensor networks are quickly gaining popularity due to the fact that they are potentially low cost solutions to a variety of real-world challenges [1]. But there are many challenges for building an application using WSN. These challenges can be divided into two main categories, traditional and recent challenges. Some of traditional challenges are:

- Low power sensing,
- Data acquisition
- wireless transmission
- Energy source
- Power management electronics

In figure 1, we just illustrate recent challenges in WSNs. During this paper we will focus only on secure routing. As seen from figure 1, one can conclude that the different tracks in WSNs are related with each other. For example, we can't work in secure routing without taking into consideration the Quality of Service (QOS). We try to develop a new routing algorithm based on AI techniques that take into account the challenges of WSN environment. The next section will discuss the Secure Routing in details.

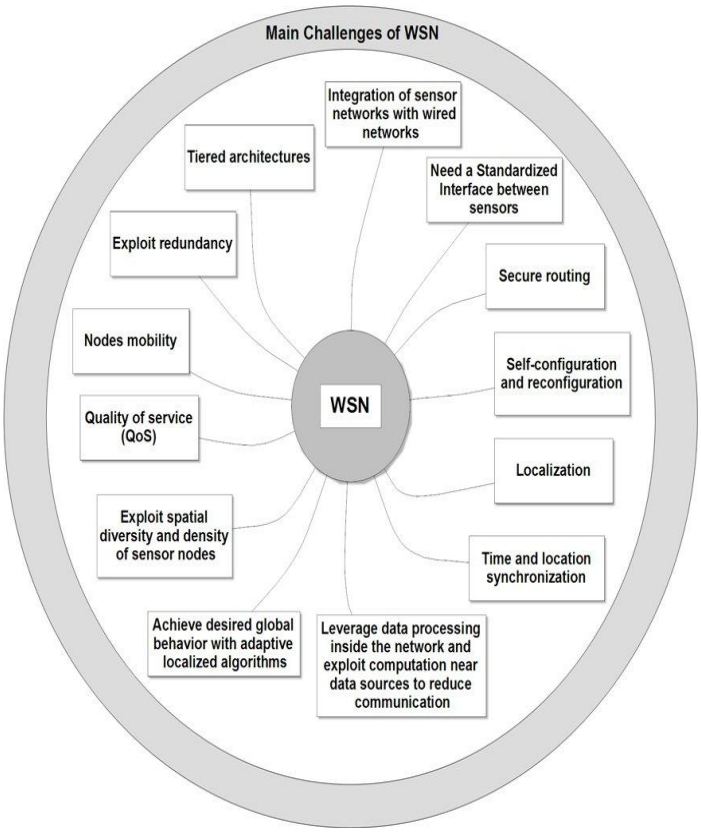

Fig 1: The Main Challenges of WSN

2. SECURE ROUTING IN WSN

Routing is the fundamental operation in WSNs that facilitates the establishment of communication links between sensor nodes and the packet delivery. Routing paths are usually established using a single path between the source and destination nodes. Therefore, availability of data and reliability of communication are a necessity [2].

There are many WSN routing protocols. These protocols try to deliver the data from a sensor to the sink node with minimum cost. Each of these protocols has its own benefits and drawbacks. The main categories of WSN routing protocols are shown in figure 2.

Based on A. Paradisi [3] study, WSN Routing Protocols – as shown in figure 2 - can be classified in four main categories based upon:

- the type of communication routes processed within the network for data transmission from the source to sink
- the type of the network structure
- the network operations carried out using these protocols
- the initiator of communications

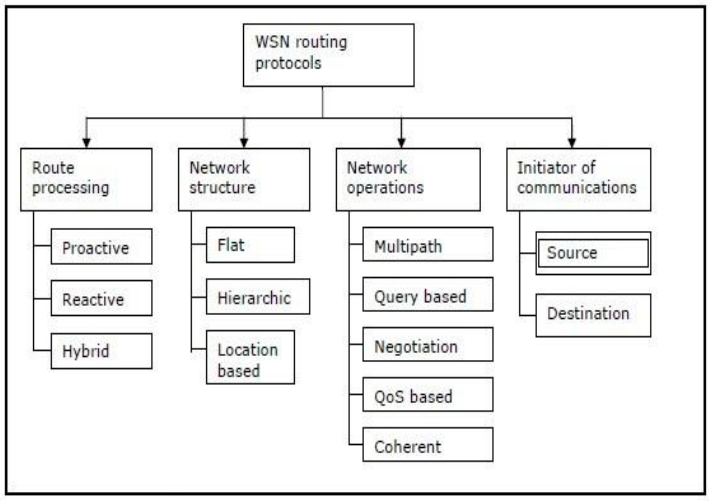

Fig 2: WSN Routing Protocol Categories

For sensitive environments, it is equally important to safeguard data from malicious activity as well as maintaining the availability and reliability of the network. Therefore, securing the routing process is a vital task to ensure the successful operation of the routing tasks.

Security aspects in routing protocols have not been given enough attention, since most of the routing protocols in WSNs have not been designed with security requirements in mind [4].

However, prior to designing secure routing protocols, one has to understand the reasons that lead to the need for security in the routing process:

- Data redundancy specially in Multipath routing.
- Routing attacks.
- Survivability
- Security not priority in routing protocol design, (mainly optimize for power (CPU / transmissions)
- Exploit redundancy around each sensor.
- Achieve desired global behavior with adaptive localized algorithms

Also we must note that, there are many types of attacks in WSN. The attack may be from outside or from inside the network. Link layer encryption and authentication mechanisms may be a reasonable first approximation for defense against mote-class outsiders, but cryptography is not enough to defend against laptop-class adversaries and insiders, careful protocol design is needed as well or there should be modification in secure routing protocol.

After finishing the literature in the WSN (WSN) security area, secure routing is related with other security issues. We must take these other issues in consideration in order to design a complete secure routing algorithm. Figure 3 shows this relationship and shows also the common types of malicious attack in WSN that faces any routing protocol:

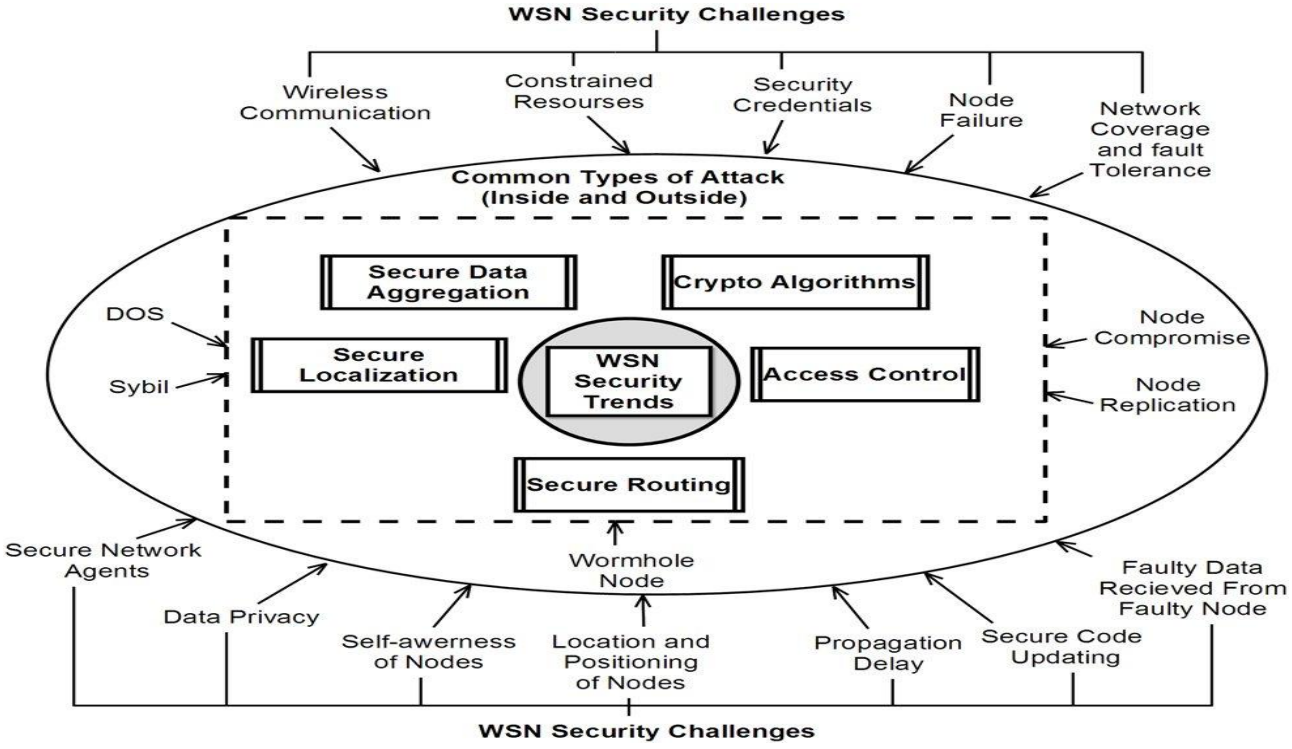

Fig 3: Security Trends for WSN.

Data aggregation aims to reduce the energy consumption by eliminating redundant data traveling back to the base station. The security issues such as data integrity, confidentiality, and freshness in data aggregation become crucial when the WSN is deployed in a remote or hostile environment where sensors are prone to node failures and compromises [5].

The problem of access control can be considered as restricting access to resources to privileged entities [6].

Localization systems can be the target of an attack that could compromise the entire functioning of a WSN and lead to incorrect decision making, among other problems . [7]. Secure localization aims to prevent the effect of any type of attacks.

Sensor networks are not inherently secure. Its nodes must be deployed near the source of the events, and they use wireless communication channels for exchanging messages. Therefore, any malicious adversary can manipulate the sensor nodes, the environment, or the communication channel on its own benefit. Besides, if that malicious outsider gains access to one or more sensor nodes, it may be possible to manipulate the information flow that traverses the nodes. Therefore, a sensor network must be prepared from the hardware of its nodes to their application layer to prevent or minimize the effect of such attacks [8].

It is indispensable to provide basic security primitives to the sensor nodes in order to give a minimal protection to the information flow and a basis to create secure protocols. Those security primitives are symmetric key encryption schemes

(SKE), public key cryptography (PKC), and hash functions. Since most sensor nodes are highly constrained in terms of resources, it is a challenge to implement them in an efficient way. These security primitives also need certain security credentials, i.e. secret keys, in order to work. The task of creating and providing these keys, hence constructing a secure key infrastructure, is done by the key management system (KMS). Constructing these KMS is not a trivial task, as they must comply with properties like scalability, communication overhead, connectivity, etc.

This underlying security infrastructure is essential for defending the network against attacks, but it is not enough to protect the entire infrastructure against attacks from the inside of the network. As a result, the most critical protocols of a sensor network must be prepared to deal with malicious activity and node failure as part of their core functionality. Routing algorithms must support full connectivity and network coverage while being fault tolerant. Data aggregation protocols must deal with false data received from faulty nodes or from nodes being controlled by an adversary. Time synchronization protocols must reduce errors must reduce errors related to malicious activity or accumulated propagation delays to the bare minimum. Finally, other protocols like clustering or location and positioning of nodes should be also as secure as possible [9].

There are other sensor network security aspects that should also be taken into account. For example, a sensor node must be able to discover any abnormal events that are occurring on its neighborhood, detecting suspicious behavior in other nodes of the network and protecting the network against any malfunctions. This self-awareness could be used as a foundation for complex security services, such as intrusion detection systems (IDS) and trust architectures. Moreover, other security aspects such as secure management of mobile nodes and base stations, delegation of tasks, data privacy, secure network agents, secure code updating, code attestation, secure random number generation, and many others, should be also considered. Note that the importance of all these security solutions must be consistent with the importance of the processed data and the security requirements of the scenario and the application [9].

3. PROBLEM STATEMENT

There are many searches that aims to secure the routing process in WSN. Each of them try to solve a fixed problem. This work gives an overview of the current state of the solutions on key issues such as secure routing, prevention of denial of key management services. WSN introduces security problems, threats, risks and other type of attacks like internal and external attacks. The first challenges of security in sensor network lie in the conflicting interest between minimizing resource consumption and maximizing security. Secondly the capabilities and constraints of sensor node hardware will influence the type of security mechanisms that can be hosted on a sensor node platform. Attacks on a WSN can target at any node. Damages can include leaking secret information, interfering messages and impersonating nodes.

As a result We need to present a intelligence based routing protocol for WSN that integrates security and reduces communication overhead by removing data redundancy from the network. The proposed protocol must provide security to the network without spending additional energy resources, particularly when we are dealing with high levels of redundancy.

4. RELATED WORK

A number of state-of-the-art reviews exist today in WSNs, covering from broad to specific areas of interest. However, a comprehensive review on secure routing issues in WSNs appears to be missing.

However, the need for secure routing in WSN applications has lead researchers to design secure routing protocols. Currently, some efforts for reviewing WSN secure routing protocols can be found in the literature. However, these reviews neither focus on all secure routing issues nor cover the method by which we can apply these issuse of existing WSN secure routing protocols.

For example, Eliana Stavrou and Andreas Pitsillides [10] have reviewed the WSN multipath routing protocols. But they have not take into consideration the attacks that can greatly influence the network when launched from inside adversaries, e.g. wormhole, sinkhole, hello attacks. These attacks are usually more difficult to defeat because the adversary has already gained access and he is considered part of the network.

After finishing the literature in WSNs secure routing, we find a few attempts to use AI algorithms in the routing process. Each of them focuses in a specific problem such as power consuming. There is no attempt to use these algorithms in order to achieve high secure and fast routing algorithm. We list here some of these attempts as the following:

4.1 WSN Routing using Swarm Technique

M. Saleema, G. Di Carob, and M. Farooqc [11] have reviewed the swarm intelligent based routing protocols in WSN and a new framework has been suggested.

The proposed framework consists of five top level modules and some additional submodules. The ensemble of these modules and submodules implements the architecture and the operations at the node router. The top level modules are: (i)

mobile agents generation and management, (ii) routing information database (RID), (iii) agent structure, (iv) agent communications, and (v) packet forwarding. Figure 4 summarizes the characteristics of the different modules and their relationships.

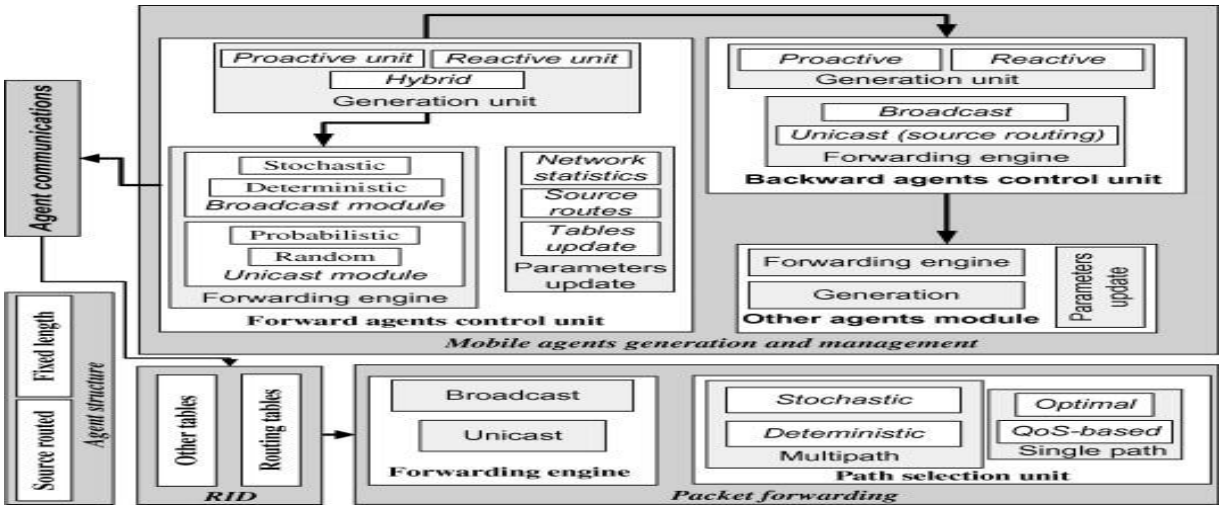

Fig 4: The common routing framework for SI routing protocols. Source: M. Saleema, G. Di Carob, and M. Farooqc [11]

This framework was designed specifically to comply with the features of WSN. From our point of view, it has two main problems: first, it is not implemented and there are no results to show its effectiveness. It just provides a proposal according to the related and previous studies but the implementation is leaved to future researchers.

The second problem is that, the security issues are not taken into account.

4.2 WSN routing using Self organizing Map (SOM)

J. Barbancho, C. Leon, F. Molina, and A. Barbancho.[12] proposed a new AI-based routing algorithm for WSN. This algorithm is called SIR which has the novelty of being based on the introduction of neural networks in every sensor node. The wireless sensor network simulator, OLIMPO, have been carried out to study the efficiency of the proposed protocol.

SIR was designed to flat-based routing network where all nodes are supposed to be assigned equal roles or functionalities. Among all the existing flat routing protocols, they have chosen directed diffusion and Energy-Aware Routing (EAR) to evaluate the influence of the use of AI techniques.

In SIR algorithm, the authors see that the best suited, among all AI techniques, is the self -organizing-map (SOM) because of the processing constraints. This kind of artificial neural network is based on the self organization concept.

From our point of view, the SIR protocol gave better results compared to other algorithms. But it is suitable only for flat-architecture of the WSN. Secondly, it is concentrated on enhancing the Quality of Service (QOS) in WSN. Thirdly, There is not enough information about whether there is a guarantee of secure routing of the data between sensor nodes or not.

Anyway, the SIR algorithm has proven that we are heading in the right direction. This can be seen through the results of the use of AI techniques for routing in WSN.

4.3 WSN Routing using Genetic Algorithms:

The "what-when-how" web site discussed the application of genetic algorithms (GA) in WSNs. The basic idea of GA was discussed and some specific considerations for WSNs were made, including crossover, mutation and definition of the fitness function. The mainly performance parameters may be divided in three groups: energy, connectivity and application specific. That work follows the cluster-based architecture of WSN. The Fitness Function Parameters are:

- Operation energy.
- Communication energy.
- Battery life.
- Sensors-per-cluster head.
- Sensors out of range error.
- Spatial density.
- Uniformity of measurement.

That work did not address the following problems: efficient routing, data aggregation, collaborative processing, sensor fusion, security, localization, data reliability, network management, etc. All these topics may benefit from the usage of genetic algorithms. The work only focused on designing the WSN using GA.

Some other researches have been made using genetic algorithms to solve some WSNs problems (Hussain, Matin & Islam, 2007) (Jin, Liu, Hsu & Kao, 2005) (Ferentinos & Tsiligiridis, 2007) (Wazed, Bari, Jaekel & Bandyopadhyay, 2007) (Rah-mani, Fakhraie, & Kamarei, 2006) (Qiu, Wu, Burns, & Holzhauer, 2006). However, most of the research topics of WSNs using genetic algorithms remain few or completely unexplored. There is no work that addresses secure routing in WSN using GA.

5. THE PROPOSED FRAMEWORK

Figure 5 shows our proposed framework. This framework determines the main phases that will be followed in order to create a new AI-based routing protocol for WSN. There are three main phases: Design phase, testing phase, and performance measure phase. Each of these steps contains a set of tasks. Each task can be understood from its name as shown.

6. CONCLUSION

Secure routing is vital to the acceptance and use of sensor networks for many applications, but we have demonstrated that currently proposed routing protocols for these networks are insecure. In this paper, we have surveyed the state-of-the-art of secure routing protocols in WSNs. We have conclude that using AI techniques in routing process is better that the traditional protocol of routing. We have also overviewed the security requirements of sensitive applications that use WSNs. The new directions and trends of WSN have been discussed. And a proposed framework for creating an AI-based routing algorithm for WSN has been declared. As future work, we plan to design and implement an AI-based routing protocol that achieve a high degree of security and takes into consideration the limitations of WSN according to our framework.

7. REFERENCES

[1] J. Jabari Lotf and S. Hossein Hosseini Nazhad Ghazan, 2011, " Overview on Wireless Sensor Networks ", Journal of Basic and Applied Scientific Research, Volume 12, issue 1

[2] K. Akkaya and M. Younis, 2005,"A survey of routing protocols in wireless sensor networks and Ad hoc Network", Elsevier Journal, Volume 3 , Issue 3

[3] A. Paradisi, 2012 , " A pedagogical platform for studying routing algorithms for Wireless Sensor Networks", Master thesis in computer sciences -Vrije university - Brussels, January

[4] E. Stavrou and A. Pitsillides, 2010, "A Survey on Secure Multipath Routing Protocols in WSNs",Computer Networks Journal, Volume 54, Issue13,.

[5] S. Desai, S. Butani and S. Valiveti, 2012,"Analyzing the Impact of Standard Encryption Approaches for Data Aggregation in a Wireless Sensor Network", International Journal of Computer Science and Telecommunications, Volume 3, Issue 6, June

[6] A.Menezes, P. Van Oorschot, and S. Vanstone, 1997, " Handbook of Applied Cryptography", CRC Press, Boca Raton, FL,.

[7] A. Boukerche, H. Oliveira, E. Nakamura, and A. Loureiro, 2008, "Secure localization algorithms for wireless sensor networks", Univ. of Ottawa, Ottawa,

[8] J. Walters, Z. Liang, W. Shi, and V. Chaudhary, 2006 , "Wireless sensor network security: a survey", in Xiao, Y. (Eds),Security in Distributed, Grid, and Pervasive Computing, CRC Press, London,

[9] R. Rodrigo, J. Lopez, 2009, "Integrating wireless sensor networks and the internet: a security analysis", Internet Research, Volume 19, Issue 2,.

[10] E. Stavrou and A. Pitsillides, 2010, " A survey on secure multipath routing protocols in WSNs", Computer Networks, Volume 54, Issue 13, September,

[11] M Saleema, G. Di Carob, and M. Farooqc, 2011, "Swarm intelligence based routing protocol for wireless sensor networks: Survey and future directions", Information Sciences, Volume 181, Issue 20, October

[12] J. Barbancho, C. Leon, F. Molina, and A. Barbancho, 2007, " Using artificial intelligence in routing schemes for wireless networks ", Computer Communications, Volume 30, No. 14-15. October,

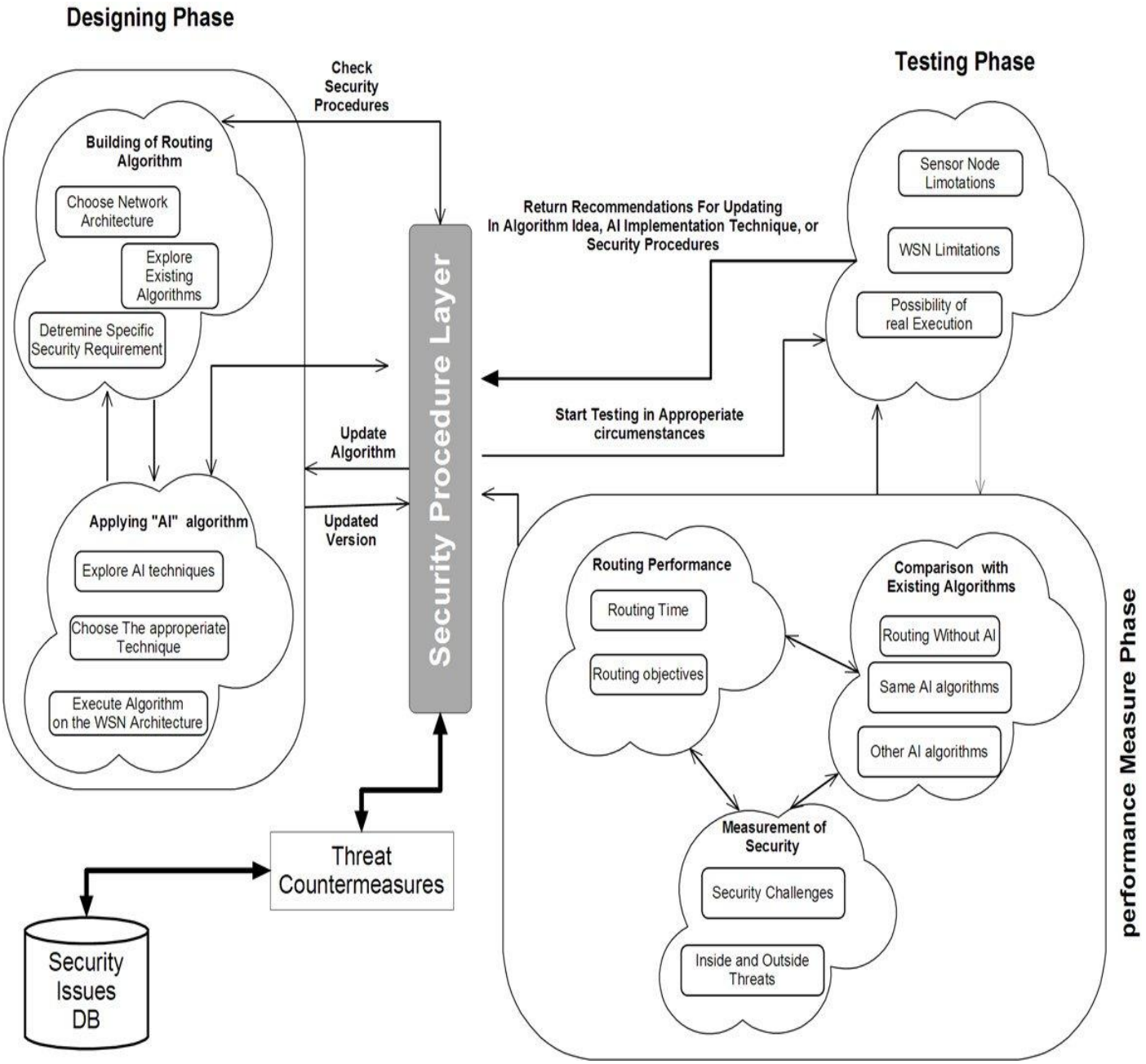

Fig 5: The Proposed Framework for AI-based Routing Protocol for WSNs.