A SURVEY ON BIO-INSPIRED SECURITY IN WIRELESS SENSOR NETWORKS

S R Mani Sekhar[1], Abhijith S[2], Bellamkonda Maruthi[3], Bharath Kumar[4], Chetan Janiwarad[5]

[1]*M S Ramiah Institute of Technology, Bangalore*
[2]*M S Ramiah Institute of Technology, Bangalore*
[3]*M S Ramiah Institute of Technology, Bangalore*
[4]*M S Ramiah Institute of Technology, Bangalore*
[5]*M S Ramiah Institute of Technology, Bangalore*

Abstract

Wireless sensor networks usually comprise of a large number of nodes which are geographically dis- tributed and are not physically connected. These nodes are frequently used to sense private data and can be necessary to transmit confidential and critical data. Hence it is important to provide security for wireless sensor networks. Research is still ongoing in this field and many models have been proposed for providing security. Looking into the symbiotic nature of biological systems can give us valuable in- sights for computer networks. Because of the analo- gies between network security and how the biotic components react to perceived threats in their sur- roundings, Bio-inspired approaches for providing se- curity in networks are interesting to evaluate . Many theories from nature such as swarm intelligence, ant colony optimisation (ACO), web spider defence, bird flocking, human immune system and so forth have been used to tackle various problems in the network- ing domain. In this paper, we intend to outline and categorize the various security attacks we encounter in a wireless sensor network and review the proposed conventional security mechanisms for them and also compare it with an alternative novel approach, i.e bio-inspired approach.

Keywords— *Wireless sensor network (WSN), Bio-inspired, security, attacks*

----------***----------

1. INTRODUCTION

Wireless sensor networks are gaining significance in the mod- ern day world because of their wide range of potential appli- cations in the fields of science, industry, transportation, civil infrastructure, and military. Communication over wireless medium is, by nature not secure and is vulnerable to vari- ous threats and attacks. Due to deployment of the nodes in physically hostile and harsh environments, multi hop and distributed architecture, WSN is more susceptible to dif- ferent types of security attacks and threats. It is easy for an attacker to launch security attacks against physical, me- dia access, or network layer in the WSN. Therefore some sort of security mechanism is highly advisable. Establishing any efficient security scheme in wireless sensor networks is made challenging by the sensors size, processing or comput- ing power of each sensor node, memory and type of tasks expected to be performed by the sensors.

In networks, security is a broad term that comprises of varied parameters like authentication, integrity, privacy, and non-repudiation [17]. A security framework in order to be agreed upon, should not violate these requirements. Al- though research in the field of sensor networks security is progressing positively, it still lacks a comprehensive inte- grated framework which can provide security to each layer and services of sensor networks. Inspired by the implicit al- luring characteristics of biological systems, many researchers are working to produce new novel design paradigms to ad- dress challenges in current network systems[14].

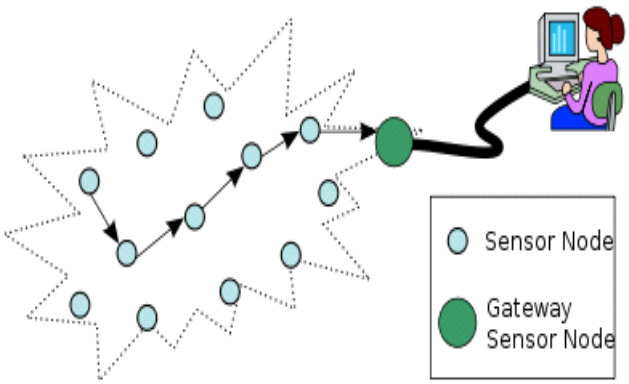

Fig 1: Nodes in WSN[7]

Adaptabil- ity, scalability, robustness are a few of many advantages that a bio-inspired approach provides. Biological techniques usu- ally are results of efforts of generations for their struggle to survive harsh conditions. Bio-inspired algorithms are built on simple rules and are usually not complex. Attacks in WSNs can be analysed from two different views. Attacks against the mechanisms which provide security (security at- tacks) to the network and attacks against basic mechanisms like routing and other physical attacks. The different types of attacks that a network can come up against are jamming, tampering, node

capture, dos attack (physical layer), col- lision (link layer), Sybil attack, wormhole, sinkhole attack, selective forwarding (network layer) and flooding (transport layer). These attacks can be negated by using security mech- anisms like effective key management, cryptography, secure broadcasting and multicasting, Intrusion detection System (IDS). The biological algorithms: ant colony optimization (ACO) is used for secure routing, spider defence mechanism, human immune system [22] are used as templates to react to the security attacks. The rest of the paper is arranged as follows. Summary of the different types of attacks in a wire- less sensor network is given in section 2. Section 3 discusses the bio inspired algorithms studied so far. In continuation to this, in Section 5 a comparison is made between conven- tional and bio-inspired approaches to securing wsns against attacks. Conclusion is given in the last section.

2. TYPES OF ATTACKS IN WSN

Here, we look at some of the attacks (discussed in the ref- erences) that tend to disrupt communications over wireless networks, and categorize these attacks based on their effects on data integrity and confidentiality, routing, identity, power consumption, privacy, and service availability and bandwidth related attacks[15].

2.1 Data Integrity and Confidentiality

2.1.1 Node Capture Attack

In Node Capture Attack, the attacker captures the sensor nodes physically and thus those nodes are compromised and the data accumulated in the nodes can be manipulated.

2.1.2 Eavesdropping Attack

In Eavesdropping attack or network sniffing, as the name suggests information is retrieved from a network by snooping on data being transmitted. The attacker is clandestinely able to overhear a private conversation in an illegitimate way.

2.1.3 Denial of Service (DoS) Attack

This attack is an attempt to make a network unavailable for its authorized users. This type attack is implemented by consuming the networks resources such as power supply, memory so that it can no longer provide its intended service. A DoS attack generally targets physical layer applications in an environment where sensor nodes are located. Jamming, Flooding and selective forwarding attacks discussed later are variations of DoS attack.

2.2 Power Consumption Related Attacks

2.2.1 Sleep Deprivation Torture Attack

This type of attack targets the link layer. The attackers target is to minimize the lifetime of the sensor nodes by in- creasing power consumption. This can be implemented by keeping the sensor nodes busy at all times depriving it of any sleep time or rest.

2.2.2 Collision Attack

In collision attack, the attacker tries to manipulate the octet configuration of transmitted packets simulating a collision. When this happens then, the packets will be discarded due to checksum mismatch.

2.3 Service Availability and Bandwidth Consumption Related Attacks

2.3.1 Flooding Attack

In this type of attack, the attacker normally sends a sub- stantial number of packets to the target node or to an access point to prevent it from establishing or continuing a commu- nication path.

2.3.2 Jamming Attack

This is a standard attack on a wireless sensor network, where a node or set of nodes are simply jammed.

2.3.3 Selective Forwarding Attack

This attack is also known as Gray Hole attack. Here, selected packets are dropped by a forwarding node other unrelated or obsolete packets are forwarded instead. The fraudulent node might also forward the message to the wrong path, creating inconsistent routing information in the network.

2.4 Routing Related Attacks

2.4.1 Wormhole Attack

In a wormhole attack or tunnel attack, an intruder manip- ulates packets at one point in the network, tunnels them to another point in the network, and then replays them into the network[26]. An attacker infringes communications from the sender, changes a portion or a whole packet, and speeds up sending the changed packet through a specific wormhole tun- nel in such a way that the altered packet arrives at the des- tination before the original packet which traverses through the usual routes.

2.4.2 Sinkhole Attack

The sinkhole attack is a severe attack that prevents the base station from obtaining complete and correct data, thus forms a serious threat to higher-layer applications. In a Sinkhole attack, a compromised node tries to draw all or as much traffic as possible from a particular area.

2.4.3 Hello Flood Attack

The routing paths are burdened (flooded) with hello or ACK messages

2.5 Identity Related Attacks

2.5.1 Impersonation Attack

An attacker impersonates another nodes identity copying the nodes MAC or IP address to enter the network or to launch other attacks on the node.

2.5.2 Sybil Attack

This is a duplication attack in which a single node provides multiple images of itself in the network when attacked. A sin- gle node presents itself to other nodes with multiple spoofed identifications (either MAC or network addresses).

3. BIO-INSPIRED ALGORITHM

Researchers over the past decade have explored nature to find a comprehensive solution to the challenges faced in the field of wireless networks. If the features of biological systems and the opposition faced by distributed network systems are studied, it is tangible to make use of bio-inspired techniques to solve these challenges[20]. Security is an aspect of concern everywhere, in nature and in the networking environment. Biologically inspired approaches for providing security in networks are interesting to evaluate because of the analogies between network security and how the biotic components react to perceived threats in their surroundings. There have been many bio-inspired approaches used as a solution to the attacks which take place in a wireless sensor network, a few of which are reviewed below:

3.1 Swarm Intelligence (SI):

The basis for swarm intelligence is the behaviour of large groups of collaborating small insects such as ants, bees or a flock of birds. Simple and seemingly unrelated, separately working individuals perform complex cooperative tasks coordinating with each other in a parallel and distributed manner[12]. Similar actions are required in networks and computer science. Thus, swarm intelligence is being used as a template for building self-organizing systems. The main focus lies on the formation of groups or clusters that allow efficient task allocation mechanisms[8].

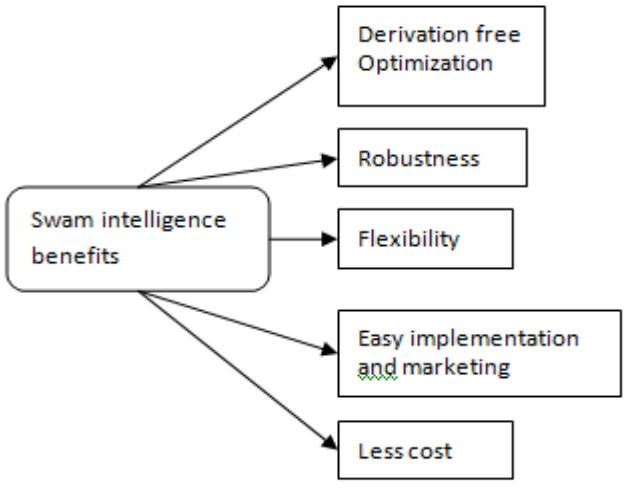

Fig 2: Swarm Intelligence

3.2 Web Spider Defence

There are various types of web spiders, a few of which use poison to paralyze their prey once it is trapped in the web[6].

This behaviour of spider, used to capture a prey by building a trap (web) can be translated into the field of networks for apprehending an attacker. This is the technique used in conventional honeypot methods.

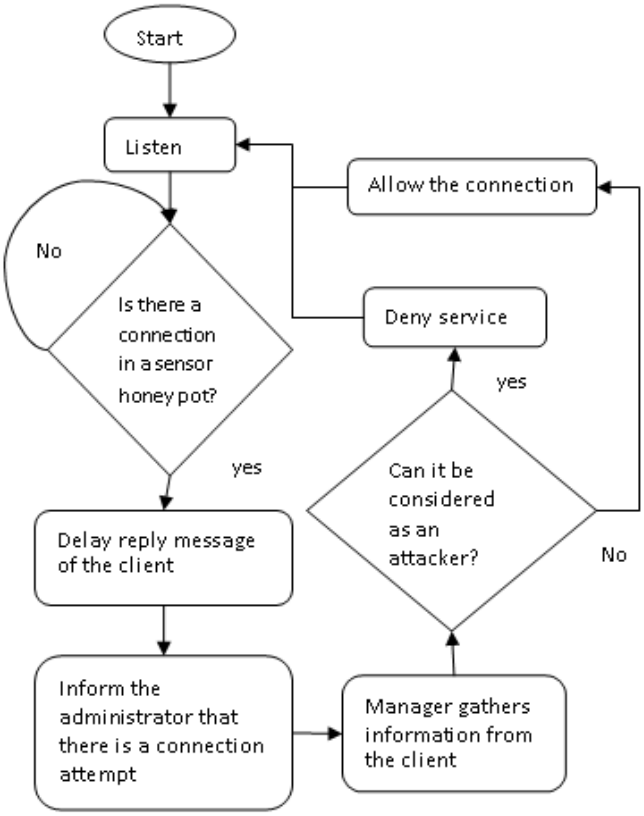

Fig 3: Web Spider Defence algorithm[6]

3.3 Ant Colony Optimization (ACO)

This comes under swarm intelligence approach, uses the organization and food transporting capabilities in large ant colonies and is widely used for solving any routing related problems in wireless networks.

Fig 4: Ant Colony Optimization (ACO)

3.4 Artificial Immune System (AIS)

The immune system in animals is the basis for artificial immune system (AIS). The immune system in animals reacts pro-actively, even to unknown attacks, and it is a highly adaptive process. The primary goal of AIS, which is inspired by the ethics and processes of the immune system, is to effectively detect changes in the environment or deviations from the normal system behaviour [9]. Therefore, it makes sense to apply the same mechanisms for self-organization and self-healing operations in computer networks.

3.5 Artificial Neural Networks (ANN)

This system is based on the organizational principles used in human brains[12].Artificial Neural Network (ANN) is a mas- sively parallel computing systems consisting of large number of interconnected simple processors to handle various types of challenging computational problem such as in wireless sen- sor network.

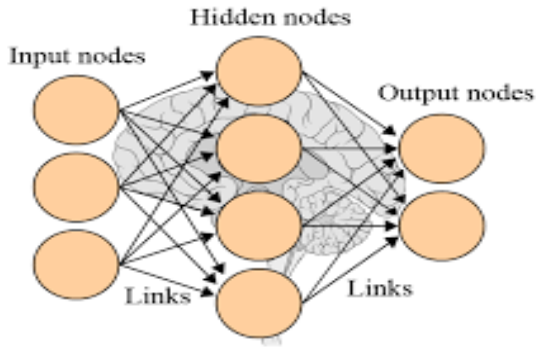

Fig 5: Artificial Neural Networks (ANN)

3.6 Human Immune System

Human Immune Systems are used as a prototype to cre- ate comprehensive and precise Intrusion Detection Systems (IDS).The inspiration for this method comes from the human body, which is composed of many cells. Out of these cells the most important are the lymphocytes (white blood cells) which have the capability to distinguish between self and non-self (foreign cells)[13].

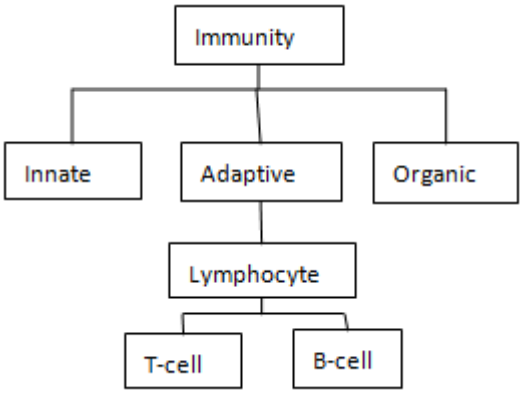

Fig 6: Human Immune System

4. SOLUTIONS TO SOME COMMON SECURITY ATTACKS IN WSN

In this section, we have tabulated a few widely accepted con- ventional and bio-inspired solutions to some of the known security threats in a wsn. Conventional security mechanisms like effective key management, cryptography, authentication, Intrusion detection System (IDS) and biological concepts such as ant colony optimization (ACO) (used for secure rout- ing), spider defence mechanism[6], artificial immune system, artificial neural network are used. The table below shows the various conventional and bio inspired approaches that have been used to solve the attacks that take place in the different layers of a OSI model.

5. COMPARISION BETWEEN CONVENTIONAL AND BIO-INSPIRED SOLUTION

5.1 Why a Bio-Inspired Solution?

When we talk about bio-inspired solution, we demonstrate a strong relationship between the security attack and biology through which we try to find a solution to the problem. The indispensable question that follows is Why is it that we need a bio-inspired solution? .The answer to this question lies in the characteristics of the biological systems such as adaptability, ability to learn and evolve when new conditions are applied, ability to self-organize in a fully distributed fashion, robustness[20]. And together with this there has also been a paradigm shift in the development of computer networks and have resulted in numerous challenges such as network topology complexity, security among others. If one looks at the characteristics of biological systems and the challenges faced by distributed network systems, it is pretty evident that one can apply bio-inspired techniques to solve these challenges[20].

5.2 Conventional Solution vs Bio-Inspired Solution

The conventional methods, mostly rely on a central processing unit (are centralized), and they depend on humans to be programmed and told what to do (and how). This has some very serious drawbacks. First, the systems are not very robust. If one part of a system goes bad, the entire system fails. Second, they are not adaptive. Most computing systems cannot adjust or adapt to new or unexpected situations without human intervention, unless mentioned in the code. Third, scalability is a bare minimum.

Table 1: summery of attacks in different layers and the se- curity mechanisms used

Layer	Attack	Conventional Security mech-anism	Bio-inspired methodology
Physical	Jamming	Direct Sequence Spread Spectrum (DSSS), Frequency Hopping Spread Spectrum (FHSS)[4]	Swarm Intelligence[3]
Physical	Node capture	Frequency Hopping Spread Spectrum (FHSS)[2]	Artificial Neural Network[11]
Network, Data Link	Sybil	Resource Testing, Random key predistribution[5]	BIOSARP Protocol based on Ant Colony System[21],Human Immune System.
Network	Sinkhole	Hop Count Monitoring method, RSSI Based Scheme[25]	Artificial Immune System (AIS)
Network	Wormhole	Packet Leashes[10], CL-MAC Protocol[1],LEACH Protocol[18]	Swarm Intelligence[19]
Transport	Flooding	Game Theory[16],Authentication, IDS	Ant Colony Optimisation (ACO)[4]
Transport, Physical, Network	DoS	Honey pot method, progressively stronger authentication, IDS	Web Spider Defence Method[6]
Transport	De-Synchronisation	Authentication, Synchronization Cookies	Artificial Neural Networks
Transport, Network	Selective Forwardingn	Support Vector Machines (SVM), Intrusion Detection System (IDS)[23]	Human Immune System[20]
Network	Hello Flood Attack	Cryptography, signal strength and client puzzles method[24]	Ant Colony System[21]

In contrast, bio-inspired (biological) methods/computing, process information in a parallel and distributed way, without the existence of a central control (decentralized). They usually consist of a large number of relatively simple individual units, each performing a part of a task. Example, the brain consists of a large number of simple neurons that are inter-connected, that process vast amounts of information. Similarly, in insect colonies, such as ants, a large number of relatively simple individuals manage to build ant hills or find a food source, in a parallel and distributed way. This paral- lel and distributed processing method makes these systems highly robust. It is easy to maintain the system. Further- more, these systems are highly scalable. Also, most systems in nature are adaptive. They can adjust to changing situa- tions or even cope with entirely new situations.

6. CONCLUSION

In this paper, we have discussed about the importance of providing security to wireless sensor networks. We categorized and gave a summary of some common attacks that a wireless sensor network encounters. A brief explana- tion was also given for each attack. Few of the biological methods/approaches that are used predominantly were reviewed. A comparison was made between conventional and bio-inspired solutions, through which we have explained the importance of bio-inspired algorithms for the optimal solutions of wsn attacks. Bio-inspired algorithms have the distinctive features of being decentralized, bottom-up, adaptable, scalable and flexible, thus providing effective solutions to problems that are otherwise restricted by limitations of conventional methods.

REFERENCES

[1]. Louazani Ahmed, Sekhri Larbi, and Kechar Bouabdellah. A security scheme against wormhole attack in mac layer for delay sensitive wireless sensor networks. Inter- national Journal of Information Technology and Com- puter Science (IJITCS), 6(12):1, 2014.

[2]. Hari Ram Tanwar Akash Jeewan, Rashid Hussain. A survey on the issues of security challenges and solutions of attacks at different layers of wsn.

[3]. Abdulaziz Rashid Alazemi. Defending wsns against jamming attacks. American Journal of Networks and Communications, 2(2):28–39, 2013.

[4]. Nabil Ali Alrajeh, Mohamad Souheil Alabed, and Mohamed Shaaban Elwahiby. Secure ant-based routing protocol for wireless sensor network. International Jour- nal of Distributed Sensor Networks, 2013, 2013.

[5]. Nitish Balachandran and Sugata Sanyal. A review of techniques to mitigate sybil attacks. arXiv preprint arXiv:1207.2617, 2012.
[6]. Alejandro Canovas, Jaime Lloret, Elsa Macias, and Alvaro Suarez. Web spider defense technique in wireless sensor networks. International Journal of Distributed Sensor Networks, 2014, 2014.
[7]. Menaka Chandra, Ankit Naik, and Chayya Chandra. Study of wireless sensor networks security issues and attacks.
[8]. Falko Dressler. Efficient and scalable communication in autonomous networking using bio-inspired mechanisms- an overview. Informatica, 29(2):183–8, 2005.
[9]. Falko Dressler and Ozgur B Akan. Bio-inspired network- ing: from theory to practice. Communications Maga- zine, IEEE, 48(11):176–183, 2010.
[10]. Mohamed Amine Ferrag and Mehdi Nafaa. An effective method of security against wormhole attack.
[11]. Hongmei He, Zhenhuan Zhu, and Erkki Makinen. A neural network model to minimize the connected dominating set for self-configuration of wireless sen- sor networks. Neural Networks, IEEE Transactions on, 20(6):973–982, 2009.
[12]. Sohail Jabbar, Rabia Iram, Abid Ali Minhas, Imran Shafi, Shehzad Khalid, and Muqeet Ahmad. Intelli- gent optimization of wireless sensor networks through bio-inspired computing: survey and future directions. International Journal of Distributed Sensor Networks, 2013, 2013.
[13]. Jungwon Kim and Peter Bentley. The human im- mune system and network intrusion detection. In 7th European Conference on Intelligent Techniques and Soft Computing (EUFIT'99), Aachen, Germany, pages 1244–1252. Citeseer, 1999.
[14]. Michael Meisel, Vasileios Pappas, and Lixia Zhang. A taxonomy of biologically inspired research in computer networking. Computer Networks, 54(6):901–916, 2010.
[15]. Aristides Mpitziopoulos and Damianos Gavalas. An ef- fective defensive node against jamming attacks in sensor networks. Security and Communication Networks, 2(2):145–163, 2009.
[16]. Raju Neyyan, Ancy Paul, and Mayank Deshwal. Game theory based defence mechanism against flooding at- tack using puzzle. In IJCA Proceedings on International Conference on Recent Advances and Future Trends in Information Technology (iRAFIT 2012), number 2, pages 35–40. Foundation of Computer Science (FCS), 2012.
[17]. ASK Pathan, Hyung-Woo Lee, and Choong Seon Hong. Security in wireless sensor networks: issues and challenges. In Advanced Communication Technology, 2006. ICACT 2006. The 8th International Conference, vol- ume 2, pages 6–pp. IEEE, 2006.
[18]. M Pushpavalli and P Mahalakshmi. Comparison of leach protocol with wormhole attack and without wormhole attack in wireless sensor networks.
[19]. Heena Rathore, Venkataramana Badarla, Sushmita Jha, and Anupam Gupta. Novel approach for security in wireless sensor network using bio-inspirations. In COM- SNETS, pages 1–8, 2014.
[20]. Heena Rathore and Sushmita Jha. Bio-inspired machine learning based wireless sensor network security. In Nature and Biologically Inspired Computing (NaBIC), 2013 World Congress on, pages 140–146. IEEE, 2013.
[21]. Kashif Saleem, Norsheial Fisal, and Sharifah Hafizah. Biosarp: biological inspired self-organized secure autonomous routing protocol for wireless sensor network. In Proceedings of the 11th WSEAS international con- ference on Applied computer science, pages 158–165. World Scientific and Engineering Academy and Society (WSEAS), 2011.
[22]. Jaime Lloret Sandra Sendra, 1 Lorena Parra and Shafiullah Khan. Review article systems and algorithms for wireless sensor networks based on animal and natural behavior. International Journal of Distributed Sensor Networks, 2015, 2015.
[23]. Bhargavi Singh. Security mechanisms for selective forwarding attack in wireless sensor networks: Review and analysis.
[24]. Virendra Pal Singh, Sweta Jain, and Jyoti Singhai. Hello flood attack and its countermeasures in wireless sensor networks. International journal of Computer Science issues, 7(11):23–27, 2010.
[25]. Chanatip Tumrongwittayapak and Ruttikorn Varakulsiripunth. Detecting sinkhole attacks in wireless sen- sor networks. In ICCAS-SICE, 2009, pages 1966–1971. IEEE, 2009.
[26]. Bing Wu, Jianmin Chen, Jie Wu, and Mihaela Cardei. A survey of attacks and countermeasures in mobile ad hoc networks. In Wireless Network Security, pages 103–135. Springer, 2007.