ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

IJARCCE

International Journal of Advanced Research in Computer and Communication Engineering

ICITCSA 2017

Pioneer College of Arts and Science, Coimbatore

Vol. 6, Special Issue 1, January 2017

A Review on Security Issues in Wireless Sensor Networks using Bio-inspired Computing

R. Kanagaraj[1], P.S. Shinu[2], K. Pavithra[3]

Assistant Professor, Dept. IT & CT, VLB Janakiammal College of Arts and Science, Coimbatore, India[1]

Student, Dept. IT & CT, VLB Janakiammal College of Arts and Science, Kovaipudur, Coimbatore, India[2,3]

Abstract: Wireless Sensor Networks (WSNs) is one of the most upcoming research area in computer science. Many issues such as clustering, routing and security problems were addressed by the latest interdisciplinary science. Now a day the Bio-Inspired Computing algorithms become more popular to solve the various issues of computer science field. Bio- Inspired Computing algorithms are the excellent behavior of the various species which is used for their life saving methods. This paper will have the review on Bio- inspired computing Algorithms which is specifically used in solving security problems in WSNs.

Keywords: WSNs, bio-inspired computing, security issues, ant colony optimization, bee colony algorithm

I. INTRODUCTION

Wireless sensor networks (WSN), sometimes called wireless sensor and actuator networks (WSAN), are spatially distributed autonomous sensors to examine physical or environmental conditions, such as temperature, sound, pressure, etc. and to cooperatively pass their data through the network to a main location. The sensor networks are composed of a large number of sensor nodes deployed densely in a closed proximity to collect data to a specific function. Sensors have limited memory, computational capability, and limited transmission capacity[11]. Complex processing and the usage of a large amount of memory are not feasible. When a large amount of sensor devices are interconnected they comprise a massively distributed system[12].

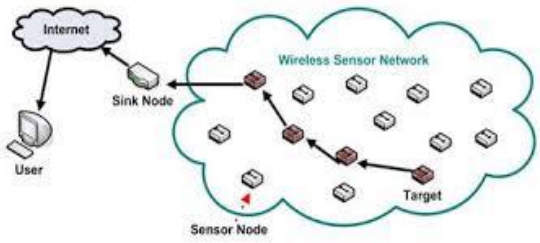

Fig.1: Security issues in Wireless networks

There is currently enormous research in the field of WSNs security. Many security solutions have been provided by using symmetric key cryptography. Some of them are given below:

Symmetric Cryptography in WSNs

The idea of the symmetric cryptography is to load secret information in the sensor nodes before their use in the network. This secret information may be the secret key itself or auxiliary information that helps the sensor nodes to derive the real secret key. With this secret key, nodes can securely communicate [13]. The main disadvantage of this solution is that compromising one node (access to the preloaded key) might lead to compromise the entire network. To overcome this limitation, several researchers propose schemes that establish pairwise keys rather than a unique global key.

In general, existing symmetric cryptographic solutions for WSNs focus mainly on the efficiency of key establishment after the deployment of the network. Furthermore, symmetric solutions do not scale well when the number of sensor nodes increases, and neglect the effect of captured node attacks. Using symmetric cryptographies in software implementation are challenging, because they are not providing a perfect trade-off between flexibility and performance, and hostile nature environments where sensor nodes are deployed makes it vulnerable to various attacks.

Asymmetric Cryptography in WSNs

Public-key cryptosystems are considered to be too heavy to use in WSNs. A pair wise key is shared between a node and each of its neighbours. A cluster key is a key shared between a node and all neighbouring nodes. A group key is a key common to the entire network. The individual key is preloaded. After deployment, neighbouring nodes establish pair wise keys. They authenticate themselves using a pre-deployed key which is erased as soon as pair wise keys are established. To establish cluster keys and the group key, nodes use broadcasts and message relaying. The protocol uses μTesla [14] to authenticate broadcasts.

Bio inspired computing

Bio-inspired computing is a field of study that loosely knits together subfields linked to the topics of connectionism, social behaviour and emergence. It is a major subset of natural computation**.** It has mainly devoted to tackle complex problems using computational methods modelled after design principles encountered in nature. Complex systems and theoretical biology are the main

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

IJARCCE

International Journal of Advanced Research in Computer and Communication Engineering

ICITCSA 2017

Pioneer College of Arts and Science, Coimbatore

Vol. 6, Special Issue 1, January 2017

foundations. It aims on understanding of the distributed architectures of natural complex systems, and how those can be used to produce informatics tools with better robustness, scalability, flexibility and which can interface more effectively with humans[15].

Bio-inspired algorithms are necessary for addressing highly complex problems to provide working solutions in time, especially with dynamic problem definitions, fluctuations in constraints, incomplete or imperfect information and limited computation capacity[16].

Ant colony optimization

The ant colony optimization algorithm (ACO) is a probabilistic technique for solving computational problems which can be reduced to finding good paths through graphs. This algorithm is a member of ant colony algorithms family, in swarm intelligence methods, and it constitutes some metaheuristic optimizations. The algorithm was aimed to search for an optimal path in a graph, based on the behaviour of ants seeking a path between their colony and a source of food. It is used to solve a wider class of numerical problems, and as a result, several problems have emerged, drawing on various aspects of the behaviour of ants[17,18]. The ants prefer the smaller drop of honey over the more abundant, but less nutritious, sugar.

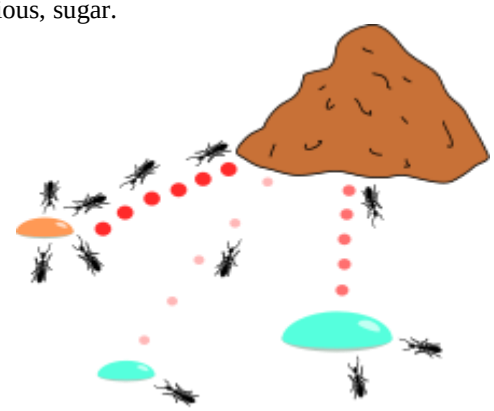

Fig. 2 Knapsack problem

Artificial bee colony algorithm

In the ABC model, the colony consists of three groups of bees: employed bees, onlookers and scouts. The artificial employed bee search for each food source. In ABC, a population based algorithm, the position of a food source represents a possible solution to the optimization problem and the nectar amount of a food source corresponds to the quality (fitness) of the associated solution. The number of the employed bees is equal to the number of solutions in the population. At the first step, a randomly distributed initial population (food source positions) is generated. After initialization, the population is subjected to repeat the cycles of the search processes of the employed, onlooker, and scout bees, respectively. An employed bee produces alteration on the source position in her memory and discovers a new food source position. Provided that the nectar quantity of the new one is higher than that of the previous source, the bee remembers the new source position and forgets the old one. After all employed bees complete the search process; the position information of the sources is shared with the onlookers. As in the case of the employed bee, it produces a modification on the source position in the memory and forms its nectar amount. Providing that its nectar is higher than that of the previous one, the bee memorizes the new position and forgets the old one. The sources abandoned are determined and new sources are randomly produced to be replaced with the abandoned ones by artificial scouts[19][20].

II . LITERATURE REVIEW

Andrea Gabrielli, Luigi V. Mancini[1] analyzed the security vulnerabilities of some well-known topology maintenance protocols (TMPs) for wireless sensor networks. It focus on increasing the duration of the sensor network by only maintaining a subset of nodes in an active or awake state. The design of these protocols assumes that the sensor nodes will be deployed in a trusted, non-adversarial environment, and does not affect the impact of attacks launched by cruel insider or outsider nodes. The proposed protocol describes the attacks that may be used to reduce the era of the sensor network, or to degrade the functionality of the sensor application by reducing the network connectivity and the sensing coverage that can be attained .Inspired by biological systems and processes, it can be taken to increase the security and fault-tolerance of the protocols.

F.Richard yu et al., [2]used cognitive radios which are able of sensing their surrounding environment and adapting their internal parameters, have been considered in mobile ad hoc networks. This deals with biologically inspired consensus-based cooperative spectrum sensing scheme in CR-MANETs. The self-organizing behavior of animal groups such as birds, fish, ants, honeybees, and others have been taken for the advancements in consensus algorithms. Contrasting the existing cooperative spectrum sensing schemes, such as the OR-rule or the 1-out-of-N rule, there is no need for a common receiver to do the data fusion for reaching the exact decision. A secondary user needs only to set up local interactions without a centralized node in CR-MANETs. Simulation is the result to show the effectiveness of the proposed scheme.

Rune Hylsberg Jacobsen et al [3], depicts about the use of biology in computer fields. Biology has often been used as a source of inspiration in computer science and engineering. Due to the appealing analogies between biological systems and large networks of small sensors Bio-inspired ideology have found their way into network node design and research. The Bio inspired principles and methods are discussed in the context of routing, clustering, time synchronization, optimal node deployment, localization and security and privacy.

Heena rathore et al[4],explores the symbiotic nature of biological systems that can result in valuable information

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

IJARCCE

International Journal of Advanced Research in Computer and Communication Engineering

ICITCSA 2017

Pioneer College of Arts and Science, Coimbatore

Vol. 6, Special Issue 1, January 2017

for computer networks. Wireless Sensor Network (WSN) is a network based on multiple low-cost communication and computing devices connected to sensor nodes which sense physical parameters. the spread of viruses in wired systems has been dealt, where the WSN is applied in an emerging research area. Security threats can be introduced in WSN through various means, similar to benevolent sensor node turning fake after a certain duration of' time. Biological inspirations and machine learning techniques are used for adding security against then arising threats. Although it uses machine learning techniques to identify the fraudulent nodes, consecutively by deriving inspiration from human immune system it effectively nullify the impact of the fraudulent ones on the network. Proposed work has been implemented in LabVIEW platform and obtained results that exhibit the accuracy and robustness of the proposed model.

S R Mani Sekhar et al.,[5] tells that Wireless sensor networks usually comprise of a large number of nodes which are purely distributed and are not connected physically. The nodes are commonly used to sense private data and can be necessary to transmit confidential and critical data. Therefore it is important to provide security for wireless sensor networks. It is interesting to evaluate as the analogies between network security and how the biotic components react to perceived threats in their surroundings. Theories from nature such as swarm intelligence, ant colony optimization (ACO), web spider defence, bird flocking, human immune system and so forth have been used to undertake various problems in the networking domain. In this paper, the authors aim to recapitulate and categorize the various security attacks that we encounter in a wireless sensor network and review the proposed conventional security mechanisms and also compare the security attacks with an alternative approach, i.e bio-inspired approach.

Salim bitam et al[6],depicts that quick advances in information and communication technologies have led to the emergence of cyber-physical systems (CPSs). Wireless sensor networks (WSNs) play a crucial role in CPSs, chiefly for surveillance and monitoring. The WSNs that are important in todays world, subject to various types of cyberattacks that can cause damage, theft, or devastation of sensitive data provided by CPSs.The author have presented a careful review of different bio-inspired techniques developed for improving cyber security of CPSs using WSNs. And also have proposed a generic bio-inspired model called Swarm Intelligence for WSN Cyber security (SIWC) that addresses drawbacks of prior bio-inspired approaches.

Haowen chan et al[7],proposed that the sensor networks offer viable solutions for a different applications. Applications like climate sensing and control in office buildings and home environmental sensing systems for temperature, light, moisture, and motion are monitored currently. Sensor networks are solution to the creation of smart spaces, which implant information technology in everyday home and work environments. The privacy and security issues posed by sensor networks have been represented as a rich field in the research. JeongGil Ko ; et al [8], proposed the confluence between the need to collect data about people's physical, physiological, psychological and behavioral processes ranging from personal to urban. The availability of the technologies that enable this data collection, wireless sensor networks for healthcare have emerged. In this review the author have presented some representative applications in the healthcare domain and describe the challenges that have been introduced to wireless sensor networks due to the required level of trustworthiness and the need to ensure the privacy and security of medical data. The challenges are exacerbated by the resource scarcity that is inherent with wireless sensor network platforms. The author outlined the prototype systems straddling application domains from physiological and activity monitoring to large-scale physiological and behavioral studies and highlight ongoing research challenges.

Ming Li et al[9],depicts that the wireless body area network is a new technology for e-healthcare that allows the data of a patient's vital body parameters and movements to be collected by small wearable or implantable sensors and communicated using short-range wireless communication techniques. Health care quality has been improved to a great potential with the help of WBAN, and thus has found a extensive range of applications from ubiquitous health monitoring and computer assisted cure to emergency medical response systems. in this article the author have keened on two important data security issues: fine-grained distributed data access control and secure &dependable distributed data storage, for sensitive and private patient medical data. various practical issues that need to be noticed while fulfilling the security and privacy requirements have been discussed by the author in this article.

Chandni et al[10],have depicted that Wireless Sensor Networks [WSN] are the networks of tiny nodes used for analyzing the intented area. Number of challenges are faced by the Developers of wireless sensor networks that arise from communication link failures and memory constraints. Many issues in WSNs are formulated as multi dimentional optimization problems ,and approached through bio inspired techniques. In this paper the author has presented some biologically inspired optimization algorithms like particle swarm optimization, bee colony optimization, ant colony optimization. These bio inspired algorithms have been applied to deal with WSN issues such as optimal deployement of nodes, their localization, network clustering and data aggregation.

III. FINDING

Here we have identified various bio-inspired algorithms and techniques to deal with different types of attacks, fault-tolerance, and for privacy. The bio inspired

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

IJARCCE

International Journal of Advanced Research in Computer and Communication Engineering

ICITCSA 2017

Pioneer College of Arts and Science, Coimbatore

Vol. 6, Special Issue 1, January 2017

Algorithms is also used to improve the accuracy and the robustness in wireless sensor networks.

IV. 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 explanation 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] Andrea Gabrielli , Luigi V. Mancini," Bio-Inspired Topology Maintenance Protocols for Secure Wireless Sensor Networks" Volume 5151 of the series Lecture Notes in Computer Science pp 399-410

[2] F.Richard yu,Minyi huang,Helen tang," Biologically inspired consensus-based spectrum sensing in mobile Ad Hoc networks with cognitive radios Volume: 24 Issue: 3"

[3] Rune Hylsberg Jacobsen, Qi Zhang and Thomas Skjødeberg Toftegaard," Bioinspired Principles for Large-Scale Networked Sensor Systems: An Overview" Received: 17 January 2011; in revised form: 21 March 2011

[4] Heena Rathore, Venkataramana Badarla, Sushmita Jha, AnupamGupta," Novel Approach for Security in Wireless SensorNetwork using Bio-Inspirations".

[5] S R Mani Sekhar1 , Abhijith S 2 , Bellamkonda Maruthi3 , Bharath Kumar4 , Chetan Janiwarad 5," ", Volume: 04 Issue: 05 | May-2015, Available @ http://www.ijret.org.

[6] Salim Bitam ; Sherali Zeadally ; Abdelhamid Mellouk," Bio-inspired cybersecurity for wireless sensor networks" (Volume: 54, Issue: 6, June 2016)

[7] Haowen Chan ; A. Perrig," Security and privacy in sensor networks" Computer (Volume: 36, Issue: 10, Oct. 2003)

[8] JeongGil Ko ; Chenyang Lu ; Mani B. Srivastava ; John A. Stankovic ; Andreas Terzis ; Matt Welsh," Wireless Sensor Networks for Healthcare", Proceedings of the IEEE (Volume: 98, Issue: 11, Nov. 2010

[9] Ming Li ; Wenjing Lou ; Kui Ren," Data security and privacy in wireless body area networks" IEEE Wireless Communications (Volume: 17, Issue: 1, February 2010)

[10] chandni,anjali bharti,jyoti," optimization through bio inspired algorithm in wireless sensor networks :survey and future directions" Volume 2,spl.issue 2(2015)

[11] Yenumula B. Reddy," trust-based approach in wireless sensornetworks using an agent to each cluster", International Journal of Security, Privacy and Trust Management (IJSPTM), Vol.1, No.1, February 2012

[12] Nessett, D. Massively distributed systems: design issues and challenges. In Proceedings of the Embedded Systems Workshop; Cambridge, MA, USA, March 29C31, 1999; USENIX Association: Berkeley, CA, USA, 1999; p. 8

[13] Y Xiao, VK Rayi, B Sun, X Du, F Hu, M Galloway, "A survey of key management schemes in wireless sensor networks", Computer Communications 30(11-12), 2314–2341, 2007

[14] Abhishek Jain, Kamal Kant and M. R. Tripathy ,"Security Solutions for Wireless Sensor Networks", Second International Conference on Advanced Computing & Communication Technologies, 2012.

[15] Luis Rocha,Santosh Manicka," biologically inspired computing"

[16] "bio inspired computing – a review of algorithms and scope of applications",volume 59, 15 october 2016, pages 20–32

[17] A. Colorni, M. Dorigo et V. Maniezzo, Distributed Optimization by Ant Colonies, actes de la première conférence européenne sur la vie artificielle, Paris, France, Elsevier Publishing, 134-142, 1991.

[18] M. Dorigo, Optimization, Learning and Natural Algorithms, PhD thesis, Politecnico di Milano, Italie, 1992.

[19] D. Dervis Karaboga, An Idea Based On Honey Bee Swarm for Numerical Optimization, Technical Report-TR06,Erciyes University, Engineering Faculty, Computer Engineering Department 2005.

[20] Jump up^ Karaboga, Dervis (2005). "An Idea Based on Honey Bee Swarm For Numerical Optimization"