IJCSE International Journal of Computer Sciences and Engineering Open Access
Review Paper Vol.-7, Special Issue, 4, Feb 2019 E-ISSN: 2347-2693

A Study of Neural Networks based Blackhole Attack Protection in WSNs

G. Vinothini

Department of Computer Science, Asst Prof in Bon Secours College for Women

Corresponding Author: Vinog7492@gmail.com

Available online at: www.ijcseonline.org

***Abstract*—** A Wireless Sensor Network (WSN) is a collection of sensor nodes, which builds up a network using radio communication in an autonomous. This spoofing technique can be executed using blackhole or sinkhole attacks, which are used to fetch the streams of data leading to cluster heads or base stations usually. In this paper, we are addressing the issue of a variant of DDoS attack: Selective-Jamming Attack as TDMA is prone to a particularly insidious form of jamming attack, namely Selective Jamming (SJ).

***Keywords*—** Blackhole, Neuralnetworks, Selective jamming, TDMA.

I. INTRODUCTION

A Wireless Sensor Network (WSN) is a collection of sensor nodes, which builds up a network using radio communication in an autonomous and distributed manner[1]. Nodes are distributed over a specific field, and are able to collect and relay information about the environment, in order to provide fine-grained observations of a phenomenon. A sensor node is typically equipped with one or more sensors that are used to capture events from the environment, an analog-digital converter, a radio transceiver, a central processing unit with limited computational capabilities, a small amount of memory and a battery power supply. Sensor devices collaborate with each other in order to perform basic operations such as sensing, communication and data processing.

Major applications using WSNs include: environmental monitoring, health care, mood-based services, positioning and animal tracking, entertainment, logistics, transportation, home and office, industrial and military applications. Non-intrusive and non-disruptive environmental monitoring helps biologists study sensitive wildlife habitats, for example the micro-climates on Great Duck Island, Maine. Health care applications enable people with certain medical conditions to receive constant monitoring through sensors. Military applications include surveillance, target tracking, counter-sniper systems and battlefield monitoring, in which information is propagated to soldiers and vehicles involved in combat.

The technological advancements in wireless networks and microelectronics had resulted in enhancing interest in the field of wireless sensor networks. A sensor network involves deploying an array of sensors for distributed monitoring of real time events. The sensor networks have limited energy, but as the sensor nodes are battery powered. These sensor nodes also have limited memory and computational capability and can be deployed in remote areas or inhospitable terrain. The use of sensor networks for life critical applications like monitoring patients in hospitals and military applications is increasing. These applications as a result make it important to have a good security system for sensor networks. The use of these networks in military applications and the limited power and memory. So to make this design of a security protocol verychallenging[1].

The security of Wireless Sensor Networks(WSN) can be compromised in many ways. A remote end user accessing base station information can be prevented from doing so in a variety of ways. Communication between the base station and sensor nodes can be blocked[13]. This can be accomplished by analog jamming of signals or by digital jamming in the form of DoS(Denial of Service) attacks that flood the network, base stations or both. Targeted DoSattacks on strategic nodes in the WSN can also block communication of large parts of the network with the base station. Communication between base stations and other sensor nodes can be prevented by setting up incorrect routing information so that traffic goes to the wrong destination or loops. One way to do this is to spoof the base

station and deceive nodes into rerouting all packets to the spoofed base station instead of the real base station. This spoofing technique can be executed using blackholeor sinkhole attacks, which are used to fetch the streams of data leading to cluster heads or base stations usually.

Another way of breaching security is to destroy the base station itself[8]. This can be accomplished by monitoring the volume and direction of packet traffic toward the base station so that the location is eventually revealed. Destruction can also be accomplished by listening to the RF signals to localize and triangulate the location of the base station. A third threat is eavesdropping. This is made easier by wireless hop-to-hop communication[2]. Eavesdropping can be used to track and deduce the location of the base station for destruction. There are many other methods to breach the WSNsecurity.

In this paper, we are addressing the issue of a variant of DDoS attack: Selective-Jamming Attack as TDMA is prone to a particularly insidious form of jamming attack, namely Selective Jamming (SJ). This kind of attack aims at disturbing communication among sensor nodes according to specific criteria and objectives. For instance, an adversary could be interested in jamming only the transmission of certain packet types, or packets sent in one specific TDMA slot of the superframe, or transmissions from a specific sensor node. Also, selective jamming could severely compromise specific traffic flows. In comparison with traditional wide-band jamming, selective jamming is more difficult to be detected, due to the reduced adversary exposure. In the following, we focus on one kind of selective jamming attack, according to which the adversary aims at disrupting communication of one specific sensor node.

II. RELATED WORK

A paper published by Marco Tilocaet. Al. proposed, "Wireless Sensor Networks (WSNs)"(2013)[1] . WSNs are presently used in many application like industrial applications and factory automation. In these Time Division Multiple Access (TDMA) is basically used for data communication between sensor nodes. As TDMA- based WSNs are prone to Selective Jamming attack in a specific form of Denial of Service(DoS) attack aimed for misuse of network reliability. In this paper, it presents SAD-SJ. It is a self-adaptive and decentralized MAC-layer solution against selective jamming in TDMA-based WSNs. SAD-SJ do not requires a central entity that needs sensor nodes to rely only on local information and allows them to join. It leaves the network without disturbing other nodes activity. We saw that SAD-SJ introduces a limited overhead, in terms of computation, communication and energy consumption."
A paper published by Md. MonzurMorshedet. Al. proposed, "Cluster Based Secure Routing Protocol (CBSRP)"(2013)[2] . MANET is a routing protocol that ensures security in key management and communication between mobile nodes. For secure communication it uses Digital Signature and One Way Hashing technique. According to CBSRP, it used in a group of small clusters that consists of 4- 5 nodes. After that, this communication takes place between mobile nodes. In a cluster, it have a cluster head. The cluster head in the cluster is not permanent. As other nodes stay queued and a new cluster node or cluster head is elected on the priority basis from the rest of the nodes. In the cluster, mobile nodes are authenticated by using One Way Hashing concept. But Digital Signature is not necessary for cluster communication. In Cluster-Cluster authentication we advised to use Digital Signatures. CBSRP ensures that secure communication will be energy efficient. We segmented the whole network into small set of clusters."

A paper published by Seuwou.P et.al. proposed " Effective Security as an ill-defined Problem in Vehicular Ad hoc Networks (VANETs)"[3].He stated vanet as technology that uses moving cars as nodes in a network to create mobile networks. VANETs enable vehicles to communicate amongst themselves (V2V communications) and with road-side infrastructure (V2I communications). Every participating car is turned into a wireless router or node, allowing connection between other cars in a radius approximately of 100 to 300 meters, thus creating a network with a wide range. In this paper he proposed various issues of effective security in VANET. He discussed various attacks in vanet , according to him the attacks are classified into two broad categories first one is physical attack which further occure due to two problems ,tamper proof device and event data recorder and another attack is logical attack which occure due to the virus , Trojan horse and protocol weakspot.

A paper published by Qian.yi et.al. proposed "Performance evaluation of a secure MAC Protocol for vehicular network"(2008)[12] In this paper he proposed an overview on a priority based secure MAC Protocol for vehicular networks and he assume that the MAC Protocol can achieve both QOS and security in vehicular networks. In this paper he proposed that the MAC Protocol is having massages with different priority for different application to access DSRC(Dedicated short range communication channel) chanel .The proposed secure MAC Protocol willuseapartofIEEE1609.2.Securityinfrastructure including PKI and ECC, the secure communication message format of vehicular networks, and the priority based channel access according to the QOS requirement of the applications.

A paper published by Javed.M.A. et.al. proposed " A Geocasting technique in an IEEE802.11p based vehicular Ad hoc network for road traffic management"(2010)[4]. In this paper he proposed the geocasting packet transmission technique to transfer safety message in a vehicular network.

He uses OPNET based simulation model to analyse the performance of proposed protocol .According to him the vanet can be seen as self organizing autonomous system which can distribute traffic and emergency information to vehicles in a timely manner.The proposed protocol select the furthest vehicle for the rebroadcast with the help of new backoff window design which reduces the number of packet transmission thus lowring the contention levels.The proposed protocol offer very low convergence and warning notification time compared to the other protocols and also generate lower broadcast overhead and packet loss ratio as compared to other protocols.

A paper published by Hung c.c. et.al. proposed "Mobility Pattern Aware Routing for Heterogeneous Vehicular Networks"(2008)[5].In this paper traditional method ad hoc routing protocols are not well suited for high dynamic network. It proposed a new Heterogeneous Vehicular Network (HVN) architecture and a mobility pattern aware routing for HVN. According to this, it HVN integrates Wireless Metropolitan Area Network (WMAN) with VANET technology. It gives better coverage in WMAN and high data rate in VANET. Vehicles in HVN can communicate with each other and can access Internet ubiquitously. It mainly focussedon the routing issue for HVN, because the routing protocol for HVN is different from MANET or VANET. They introduce the Mobility Pattern Aware Routing Protocol (MPARP) for HVN to provide more reliable V2V service. According to this protocol the 802.16 is used as the base station which keeps information table The table includes each vehicle's id, current position, and current speed. It will update whenever there is a position update for any of the members in the table. This protocol uses some format for sending messages.

A paper published by Dias .A.J. et.al. proposed "Testbed-based Performance Evaluation of Routing Protocols for Vehicular Delay-Tolerant Networks"(2011)[6]. This paper presents a testbed performance evaluation of DTN-based routing protocols applied to VDTNs(vehicular delay tolerant networks). The objective is to evaluate and understand how popular routing strategies perform in sparse or partitioned opportunistic vehicular network scenarios. This paper based on Spray and Wait protocol. The idea behind using this protocol is to exploit the physical motion of vehicles and opportunistic contacts to transport data between disconnected parts of the network. According to proposed protocol the buffer size and bandwidth is reduced because this protocol manages the flooding by sending single copy of message but suffer from long delivery delay.

A paper published by Sumra A.I. et.al. proposed "Trust Levels in Peer-to-Peer (P2P) Vehicular Network"(2011)[8]. In this paper key component of security in vehicular application if any component behave unexpectedly is trust. It might be harmful for other users of the network. In this they are proposed three different trust levels in peer to peer vehicular network. Its Purpose is to discuss the functionality of different components of network that circumvents the attacker. It emphasizes on the role of trusted users in peer to peer vehicular communication. According to this, Trust is combination of expectancy. It believes in expectancy and willingness to be vulnerable for that belief. This divides the trust in three levels as: zero trust level, weak trust level, strong trustlevel.

A paper published by Ghaleb F. et.al. proposed " Security And Privacy Enhancement In VANETs Using Mobility Pattern"(2013)[13].This paper is presenting a mobility pattern based misbehavior detection approach in VANETs. According to this paper the attackers can be classified as insider and outsider. Insider is a legitimate node might intentionally or unintentionally make unauthorized or undesirable actions (Misbehavior), such as modify, fabricate, drop the messages in addition to, impersonate other node identities. Outsider, on the other hand, is a kind of intruder aim to intercept, misuse ordenial of the communications among VANET's nodes. Misbehavior in VANETs can be viewed two perspectives:(i) physical movement and

(ii) information security perspectives. Anonymous Location-Aided Routing for MANET (ALARM) is used for vehicular network which relies on the location information and corresponding time. This paper includes algorithms by which the misbehavior can be detected.

(iii) A paper published by Sharma G. et.al proposed "Security Analysis Of Vehicular Ad Hoc Network (VANET)" (2010) [10]. In this paper various type of security problems and challenges of VANET been analyzed and discussed; author of this paper also discuss a set of solution to solve these challenges and problems. According to this paper each vehicle has OBU (On Board Unit).this unit connects vehicles with RSU via DSRC. and another device is TPD(Tamper Proof Device),this device hold the vehicle secrets like keys, drivers identity, trip detail, route, speed etc. Various attacks discussed are DOS, Fabrication Attack, Alteration Attack, Replay Attack and various attackers are Selfish Driver, Malicious Attackers, Pranksters. According to this paper Various vehicular network challenges are Mobility, Volatility, Privacy VS Authentication, Privacy VS Liability, Network Scalability and various security requirements are Authentication, Availability, Non repudiation, Privacy, Integrity , privacy, Confidentiality.

III. PROBLEM STATEMENT

Wireless Sensor Networks (WSNs) are recently used in many application such as industrial applications and factory automation. In these Time Division Multiple Access (TDMA) is typically used for data communication among sensor nodes. However, TDMA-based WSNs are prone to blackhole attacks which can stop the whole communication between sensor nodes or sensor nodes and cluster heads or cluster heads and base stations. In the existing paper, authors have presented SAD-SJ (Self-Adaptive Decentralized solution against Selective Jamming) WSN protocol, a self-adaptive and decentralized MAC-layer solution against selective jamming in TDMA-based WSNs. SAD-SJ is an effective WSN secure protocol against selective jamming attach, a specific form of Denial of Service attack, requires sensor nodes to rely only on local information, and allows them to join and leave the network without hindering other nodes activity. But this protocol is not capable of protecting against blackhole. In order to address blackhole attack neural networks technique can be used to protect against this attack.

IV. METHODOLOGY

At first stage, a detailed literature study would be conducted on the blackhole attacks and existing solution for WSNs. Literature study will lead us towards refining the structure of the proposed security solution design. Afterwards, the proposed solution will be implemented in NS2 simulator and a thorough performance analysis would be performed. Obtained results would be analyzed and compared with the existingtechniques.

We will start our research project by conducting a detailed literature review on the blackhole attack in case of WSNs to know the problem in detail. Then, a detailed security mechanism would be designed to prevent the blackhole attack. The simulation would be implemented using MATLAB. The obtained results would be examined and compared with the existing security mechanism to address the similar issues. Waterfall development method is ideal for projects with clear task formalization and fixed scope of work like this research work, i.e. for small and medium-size projects.

Waterfall methodology comprises the following steps:

- working out system requirements, drawing up and approving thespecification;
- design andprototyping;
- development;
- delivery;
- analysis and finalization.

V. CONCLUSION AND FUTURE SCOPE

In the research project, we propose a new security mechanism based on neural networks make the sensor nodes capable of protecting against the blackhole attack. Artificial neural networks are computational models inspired by animals central nervous systems(CNS) which is capable of machine learning and pattern recognition. These properties of neural networks will be used to enhance the WSN nodes working to protect against blackhole attacks. The neural network will generate multiple random unique codes and add them to the inter communication packets, at the sender's side. On the receiver side, these unique codes will be verified using the unique code verification calculation method. This will protect the nodes by discarding the non-matching packets from external nodes attempting to launch blackhole attack.

REFERENCES

[1] Marco Tiloca, Domenico De Guglielmo, GianlucaDini and Giuseppe Anastasi, "SAD-SJ: a Self-Adaptive Decentralized solution against Selective Jamming attack in Wireless Sensor Networks", ETFA, vol. 18, pp. 1-8, IEEE,2013.

[2] Md. MonzurMorshed, Md. Rafiqul Islam, "CBSRP: Cluster Based Secure Routing Protocol", IACC, vol. 3, pp. 571-576, IEEE,2013.

[3] Patrice Seuwou, Dilip Patel, Dave Protheroe, George Ubakanma "Effective Security as an ill-defined Problem in Vehicular Ad hoc Networks (VANETs)".

[4] Muhammad A. Javed and Jamil Y. Khan "A Geocasting Technique in an IEEE802.11p based Vehicular Ad hoc Network for Road Traffic Management".(2010).

[5] Chia-Chen Hung, Hope Chan, and Eric Hsiao-Kuang Wu "Mobility Pattern Aware Routing for Heterogeneous Vehicular Networks"(IEEE WCNC 2008).

[6] JoãoA. Dias, João N. Isento, Vasco N. G. J. Soares, FaridFarahmand, and Joel J. P. C. Rodrigues "Testbed-based Performance Evaluation of Routing Protocols for Vehicular Delay-Tolerant Networks" (2011IEEE).

[7] Steffen Moser, Simon Eckert and Frank Slomka "An Approach for the Integration of Smart Antennas in the Design and Simulation of Vehicular Ad-Hoc Networks" 2012 IEEE.

