International Journal of Innovative Research in Technology & Science
Received 7 August 2018, Received in revised form, 18 August 2018, Accepted 22 September 2018, Available online 30 September 2018
ISSN: 2321-1156 Volume VI Issue V, September 2018

An IDS Security Against Energy Consumption Vampire Attack In WSN

Amit Patle, Department of CSE, TITS, RGPV, Bhopal, India; patleamit.patle98@gmail.com;
Neetesh Gupta, HOD in CSE, TITS, RGPV, Bhopal, India; Gupta_neetesh81@yahoo.com;

ABSTRACT

The sensor nodes in network play an important role of communication in restricted battery provide called node energy or power. The proposed Intrusion Detection System (IDS) is a reliable protection scheme to provide the entire security from Vampire attacks that flooded the unwanted packets and consuming bandwidth and node energy. Therefore the proposed IDS secure routing provides higher and trustful network performance. The aggressor is also affected the limited energy resource. In this paper the center of consideration is on the safety issues relating to WSN routing protocols. The IDS is first watch the attacker flooding quantity and identified the vampire attacker and also measures the energy consumption with respect to data receiving and found that the energy consumed by attacker with available bandwidth capacity. The flooding of attacker is increases according to time but the messages are not provides any useful information. The proposed IDS is secure and provides the better performance than previous trust based security scheme in ESN.

Keywords: - WSN, Vampire Attack, Energy, Bandwidth, Routing, Security, IDS. Introduction

INTRODUCTION

Wireless sensor Networks (WSNs) incorporates spatially distributed autonomous little devices that hand and glove monitor environmental or physical conditions in remote and infrequently hostile environments. Because of recent technological advances, the producing of little and low price sensors became technically and economically possible. The sensing natural philosophy live close conditions associated with the setting close the sensing element and transform them into an electrical signal. Process such a signal reveals some properties regarding objects situated and/or events happening within the vicinity of the sensing element. An outsized range of those disposable sensors are often networked in several applications that need unattended operations. A Wireless sensing element Network (WSN) contains tons of or thousands of those sensing element nodes. These sensors have the flexibility to communicate among each other or to external base-station (BS). A larger range of sensors permits for sensing over larger geographical regions with more accuracy. Wireless sensing element Networks (WSN) [1] consists of various little sensors deployed at high density in regions requiring surveillance and observance. The sensing elements are deployed at a price abundant below the normal wired sensor system. An oversized range of sensors deployed can modify for correct measurements. A sensing element Node consists of one or more sensing components (motion, temperature, pressure, etc.), a battery, and low power radio trans-receiver, silicon chip and restricted memory, mobilizer (optional), a position finding system. A very important side of such networks is that the nodes are unattended, have restricted energy and therefore the constellation is unknown. Several style challenges that arise in sensing element networks area unit because of the restricted resources they need and their deployment in hostile environments. A Wireless sensing element Network (WSN) may be a specific sort of Ad hoc network. The taking part nodes are sensible sensors that are sensing the neighbors, equipped with advanced sensing functionalities (thermal, pressure, acoustic, etc.), a little processor, and a short-range wireless transceiver [2]. The nodes switch over information so as to make a world read of the monitored region Figure 1. This information is usually created accessible to the user through one or more gateway nodes [3]. Basically, the sensor nodes having comprise sensing, processing, communication, mobilizes, location finding system, and power units. The identical figure shows the communication design of a WSN. sensing element nodes area unit sometimes scattered in a very sensing element field, that is an area unit, a neighborhood, a district, a region, a locality, an area, a part and a section wherever the sensing element nodes are deployed. Sensing nodes coordinate among themselves to provide high class info regarding the physical setting. Every node bases its selections on its operation, the data it presently has, and its information of its neighbors. The nodes in sensor network are free to move at any place because of that the nodes are easily affected from attacker [4]. The attacker is only degrades the performance of network.

ROUTING PROTOCOLS IN WSN

Routing in wireless sensor network (WSN) differs from conformist routing in fixed networks in various ways. The sensor node done routing without any fixed infrastructure, wireless links are unreliable, sensor nodes possibly will fail, and routing protocols have to congregate stringent resources requirements [5, 6, 7]. Routing paths can be established in one of three ways, namely proactive, reactive or hybrid.

Proactive (table-driven) Routing Protocol

The proactive routing protocol is the table driven protocol to managing the table of route information in network. The proactive routing protocol are showing the better performance in fixed or stationary network because the routing table updation is not possible their but in dynamic sensor network the routing information is changes by that the overhead in network is more. The most well-known types of the proactive routing protocol are: - Destination sequenced distance vector (DSDV) routing protocol

Reactive (on-demand) Routing Protocol

The reactive routing protocols re maintaining the connection in an on demand manner means if required then established connection. The routing protocol are flooded the route request and if the destination found data delivery is started but after the

Received 7 August 2018, Received in revised form, 18 August 2018, Accepted 22 September 2018, Available online 30 September 2018
ISSN: 2321-1156 Volume VI Issue V, September 2018

completion of routing procedure including data sending route information is completely destroyed in from nodes that has participating in routing. The Ad hoc on-demand distance vector (AODV) and Dynamic source routing (DSR) protocol is the example of that kind of routing

Hybrid Routing Protocol

The hybrid routing protocol as the name suggests have the combine advantages of proactive routing and reactive routing to overcome the defects generated from both the protocol when used separately. Design of hybrid routing protocols are mostly as hierarchical or layered network framework. In this system initially, proactive routing is employed to collect unfamiliar routing information, and then at later stage reactive routing is used to maintain the routing information when network topology changes. The familiar hybrid routing protocols are: - Zone routing protocol (ZRP) [8].

SECURITY THREATS IN WSN

It defines the intrusion as any set of actions that are attempting to compromise the main components of the security system

1) The integrity,

2) Confidentiality or availability of a resource.

In the same work, the intruder therefore was defined as an individual or group of individuals who take the action in the intrusion. The plainness of many routing protocols for wireless sensor networks makes them an easy target for the attacks. The [9, 10, 11, 12] are classifies the routing attacks into the following categories;

Spoofed, Altered, or Replayed Routing Information

While sending the data, the information in transition may be spoofed, altered, replayed, or destroyed. Due to the short range transmission of the sensor nodes, an attacker with high processing power and larger communication range could attack several sensors simultaneously and modify the transmitted information.

Selective Forwarding

In this kind of attack a malicious node may decline to forward every message it gets, acting as black hole or it can forward some messages to the wrong receiver and simply drop others.

Sinkhole Attacks

In the Sinkhole attack, the goal of the attacker is to attract all the traffic. Especially, in the case of a flooding based protocol the compromised node may listen to requests for routes, and then reply to the requesting node with messages containing a bogus route with the shortest path to the requested destination.

Sybil Attacks

In Sybil attack the malicious node presents itself as multiple nodes. The attack of this type tries to degrade the usage and the efficiency of the distributed algorithms that are used. Sybil attack can be performed against distributed storage, routing, data aggregation, voting, fair resource allocation, and misbehavior detection [11].

Wormholes

Wormhole attack [12] is an attack in which the malicious node tunnels messages from one part of the network over a link, that doesn't exist normally, to another part of the network. The simplest form of the wormhole attack is to convince two nodes that they are neighbors. This attack would likely be used in combination with selective forwarding or eavesdropping.

HELLO Flood Attacks

This attack is based on the use by many protocols of broadcasting Hello messages to announce themselves in the network. So an attacker with higher range of transmission may send many Hello messages to a large number of nodes in a big area of the network. These nodes are then convinced that the attacker is their neighbor. Consequently the network is left in a state of confusion.

Acknowledgement

Some wireless sensor network routing algorithms require link layer acknowledgements. A compromised node may exploit this by spoofing these acknowledgements, thus convincing the sender that a weak link is strong or a dead sensor is alive.

Vampire Attack

A particularly Vampire attack is the attack, where a malicious node forces legitimate nodes to waste their energy by resisting the sensor nodes from going into low power sleep mode. The goal of this attack is to maximize the power consumption of the target node, thereby decreasing its battery life. So, it is also known as battery exhaustion attack.

SECURITY SCHEMES IN WSN

Security schemes are providing the free environment from malicious nodes to do malicious activities and then identified the attacker presence in network.

Amee A. Patel, Sunil J. Soni [13], the proposed approach aim to supply a mechanism that is employed to find the vampire attack in WSN. Vampire attacks are often outlined because the transmission and composite on of a message that causes additional energy to be consumed by the network than if an honest node transmitted a message of identical size to an equivalent destination. They tend to discuss the result of Vampire attacks on Ad-hoc On Demand Vector Routing (AODV). AODV may be a reactive protocol that maintains routes solely between nodes which require communicating. The routing messages don't contain info concerning the complete route path, however solely concerning the supply and destination.

Chen Hongsong, Han Zhi, Fu Zhongchuan (2015) a unique trust routing theme is proposed. Multi-agents collect multi-factors info and get together to make your mind up the trust route. Trust is that the degree of belief concerning the long run behavior of alternative entities, that relies on the past expertise of the nodes. To device network, if WSN nodes wish to speak or exchange key information, it's necessary to ascertain trust relationship between nodes to make sure the reliable information exchange. Trust is expounded to several factors, similar to hop count node behavior node's residual energy. To enhance security and dependability in device network, trust routing theme is projected within the paper. Trust is often taken as belief, reputation, likelihood, and trait. Trust routing reflects the

Received 7 August 2018, Received in revised form, 18 August 2018, Accepted 22 September 2018, Available online 30 September 2018
ISSN: 2321-1156 Volume VI Issue V, September 2018

trustworthy degree of routing path. In device network, additionally to the standard hop count, routing trait is expounded to several factors, similar to node's residual energy node's attack behavior.

Miss. Prachi, S. Moon, Mr. Piyush, K. Ingole (2015) we've analyzed a collection of algorithms put together referred to as CAWS and MES-1. CAWS (cellular automata primarily based security algorithms) [12], which incorporates key management below cellular automata rule and secure digital communication rule, that need less quantity of memory and fewer quantity of easy computation. Modern Encryption Standard (MES-1) [12] is a sophisticated cryptography technique that is employed for double cryptography and coding. Modern Encryption Standard (MES-1), the strategy is achieved by file splitting into 2 elements, that is encrypted and encrypting the divided section of the go in totally different kind by victimization cipher technique similar to TTJSA and DJSA cipher techniques. These strategies are accustomed take a look at on totally different files. Modern Encryption Standard (MES-1) is essentially used for sturdy cryptography technique. This cryptography commonplace is usually accustomed code and decodes information for security purpose in network in order that info ought to firmly transmit from supply to the destination with success.

Lina R. Deshmukh, Prof. A. D. Potgantwar (2015) first of all targets to judge these vulnerabilities to routing layer battery reduction attacks. Second it focuses upon the amendment in an existing routing protocols to certain loss because of vampire attacks at the time of forwarding of packets. Here third side, targets to surface outcomes measuring the expediency of varied representative protocols in existence of a personal vampire. It's the supply routing, distance vector, link-state, and beacon routing protocols additionally a logical ID-based device network routing protocol have shown the consequences of Vampire attacks.

Kashif Saghar, David Kendall, Ahmed Bouridane (2015) is targeted on one such attack referred to as hello flood attack. Some WSN routing protocols needs the nodes to announce themselves to neighbor nodes employing a 'Hello' message. This message permits the receiver nodes in neighborhood which will hear this message, to assume that the sender is among their radio vary. This can be an easy means of initializing a device network. However, there's a drag during this straightforward mechanism as this results in salutation flood attacks. The main aim of RAEED is secure and economic output in presence of various DoS attacks together with the salutation flood attack.

Raja Waseem Anwar, Majid Bakhtiari, Anazida Zainal, Abdul Hanan Abdullah and Kashif Naseer Qureshi (2015) they propose a trust aware distance vector routing protocol (T-AODV) to protect wireless sensor network from wormhole attacks. Through experimental results, their propose approach tested the network efficiency in terms of improved packet delivery fraction, end-to-end delay and vary of node to the destination.

Eugene Y. Vasserman and Nicholas Hopper (2013)"Vampire Attacks: exhausting Life from Wireless ad hoc device Networks" This title explores resource depletion attacks at the routing protocol layer, that permanently disable networks by quickly exhausting nodes' battery power. These "Vampire" attacks don't seem to be specific to any specific protocol, however rather trust the properties of the many widespread categories of routing protocols. The discover that each one examined protocols are vulnerable to vampire attacks, that are devastating, troublesome to find, and are simple to hold out victimization as few united malicious business executive causation solely protocol-compliant messages. Within the worst case, one vampire will increase network wide energy usage by an element of O (N), wherever N within the range of network nodes. They tend to discuss strategies to mitigate these styles of attacks, together with a replacement proof-of-concept protocol that demonstrably bounds the injury caused by Vampires throughout the packet forwarding phase.

PROPOSED IDS AGAINST VAMPIRE ATTACK

WSN contains one large number of sensor nodes, organized in a random manner. Each sensor node has limited resources of power, memory, processing and communication capabilities and functions in unattended manner. All sensor nodes monitor the environment and send sensed data periodically in a hop-by-hop manner towards the destination using the same radio channel. The attackers in network continuously deliver the huge amount of packets in network at different time interval this kind of behavior of attacker are called Vampire attack. This attack are consumes the whole bandwidth of network by that nodes are not deliver the any information in network. In this paper we develop a new profile based scheme for protecting network from Vampire attack. Sensor nodes are usually powered by small batteries or in some cases they could draw power from the environment, possibly by the use of small solar panels, motion generated power, etc. This limits the amount of power resources at hand. Wireless sensor networks could be placed in inhospitable environments, which make the replacements of batteries impossible. These limited power resources are used for sensor operations, sensor data processing and communication.

Wi: Wireless Sensor Nodes // i =0, 1, 2, 3.....n for all where i exist

Si: Represents sender nodes // Si ϵ Wi

Di: Number of Receiver nodes // Ri ϵ Wi

Ii: Intermediate Nodes // Ii ϵ Wi

Routing protocol = AODV // Ad hoc On Demand Distance Vector

Ei: Energy of Nodes // Consider energy initial level randomly

Vi: Vampire Attacker Nodes

IDS: IDS or Prevention node

Step 1 IDS capture all nodes Ii information, Vi abnormal status, Node ID, Energy information of Abnormal Node)

{

Step 2 If (IDS receives malicious information through Vi neighbor)

{

Directly communicate to attacker for update unfaithful status;

International Journal of Innovative Research in Technology & Science
Received 7 August 2018, Received in revised form, 18 August 2018, Accepted 22 September 2018, Available online 30 September 2018
ISSN: 2321-1156 Volume VI Issue V, September 2018

If (Status of Vi != Update) // means only flooding
Flooding is only produce in presence of attacker
}
Step 3 Broadcast Vi malicious activity to all alive nodes
Step 4 Block the Vi attacker node // block through off their communication
}
Step 5 Else if (Status of Vi = = Normal)
{
Path is future established
Identified attacker node by IDS
}
}
}
Stop

The proposed scheme is directly identified the basic behavior of actual routing and the routing is affected from attacker. In existing approach the only attacker performance is identified through unwanted flooding of data and consumption of energy. The energy consumption is good but also the data packets are delivered at destination in sufficient amount of quantity.

SIMULATION RESULTS

In this section evaluates the network performance in presence of attack, existing scheme and proposed IDS security in WSN.

PDR Analysis

The successful data receiving percentage with respect to sending is calculated through PDR metrics in network. The flooding of attacker is definitely degrades the receiving of data because of that the PDR performance is definitely showing the degradation in performance. In presence of Vampire attacker the lowest performance is about 15% and highest is about 45% at the starting time of simulation is measure but after applying proposed IDS the packets successful percentage is enhanced in both the security scheme. In proposed IDS scheme the successful packets receiving is reaches more than 95% and in existing performance is about 90% up to end of simulation time.

Throughput Performance Analysis

The successful packet receiving is also shoeing the better throughput performance because if the data is properly receiving then the packets receiving in per unit of time is also more. In this graph the performance of proposed IDS is again gives the better results that showing the improving in routing performance. In this graph the maximum throughput in presence of IDS is about more than 2100 packets/seconds but in presence of Vampire attack throughput performance is almost count negligible. The performance of IDS is better than the existing security scheme in IDS the same route establishment conditions are change and changeable condition are in favour of security scheme in WSN.

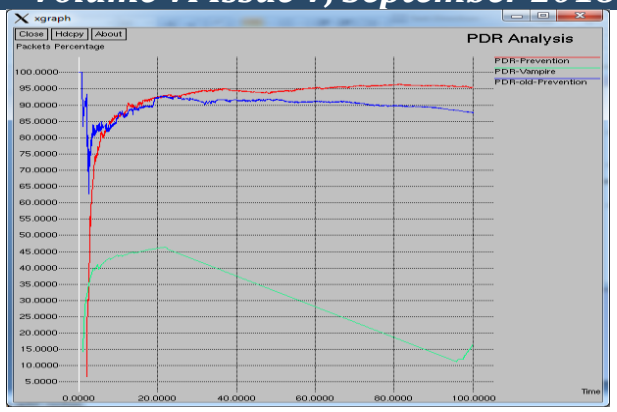

Fig.1 PDR Analysis

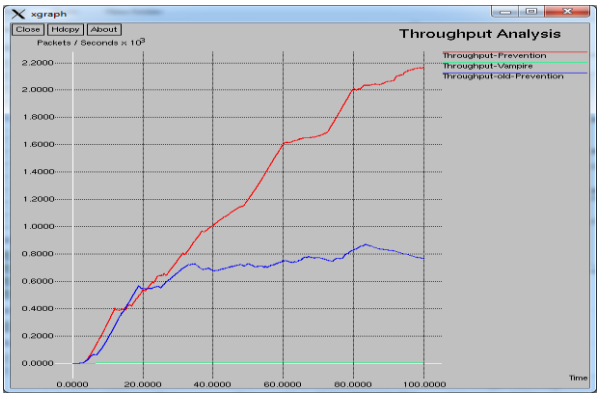

Fig.2 Throughput Analysis

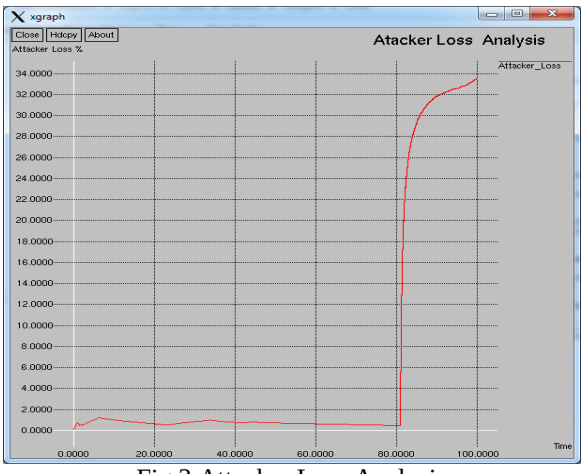

Fig.3 Attacker Loss Analysis

Attacker Percentage Loss

Vampire attack consumes the energy of normal nodes and decreases the performance of the network and while more node energy is utilized for fewer packets receiving then network split in number of sub network and increase the network overheadIn this graph performance of only attacker loss is measured and identified that the up to end of simulation time 100 seconds about 34% are drop due to presence of attacker but after applying IDS scheme not a single packet is drop due to attacker infection in sensor network.

Received 7 August 2018, Received in revised form, 18 August 2018, Accepted 22 September 2018, Available online 30 September 2018
ISSN: 2321-1156 Volume VI Issue V, September 2018

CONCLUSION AND FUTURE WORK

The Intrusion Detection System is able block the attacker malicious activities and provides secure communication. The routing protocols in WSN are fairly anxious because attackers or malicious nodes will simply acquire data regarding network topology at the time of route establishment. The proposed IDS security is reliable and more effective than the previous existing scheme in WSN. The number of nodes having affected from Vampire flooding is also loss their limited energy resource that showing the degradation in performance. The throughput, PDR performance in presence of attacker is very poor and after applying proposed IDS it again gaining the height of better performance. The various author recent works is extremely effective and distinctive but proposed security is reliable and produces less overhead to improve routing performance. The extra flooding is very harmful for the proper data deliver or communication. The proposed scheme is completely stop the flooding by disable attacker.

In future we proposed the congestion control scheme to reduce the data loss and this scheme is check the reliability of data loss. Here proposed scheme will also identified the packet dropping attacker like black hole or wormhole is detected on this manner.

REFERENCES

[1] Chris Karlof, David Wagner, “Secure Routing in Wireless Sensor Networks", Attacks and Countermeasures”, Ad Hoc Networks (Elsevier), Page: 299-302, 2003.

[2] Santi, P. “Topology control in wireless ad hoc and sensor networks” Chichester, England: John Wiley & Sons, 2005.

[3] Jun Zheng and Abbas Jamalipour, “Wireless Sensor Networks: A Networking Perspective”, a book published by A John & Sons, Inc, and IEEEE, 2009.

[4] P. Mohanty, S. A. Panigrahi, N. Sarma, and S. S. Satapathy, “Security Issues in Wireless Sensor Network Data Gathering Protocols: A Survey” Journal of Theoretical and Applied Information Technology, pp. 14-27, 2010

[5] 8Clement Ogugua Asogwa, Xiaoming Zhang, Degui Xiao, Ahmed Hamed, “Experimental Analysis of AODV, DSR and DSDV Protocols Based on Wireless Body Area Network” Communications in Computer and Information Science, Springer-Verlag Berlin Heidelberg, Volume 312, pp 183-191, 2012.

[6] 9Faleh Rabeb, Nasri Nejah, Kachouri Abdennaceur, Samet Mounir, “An Extensive Comparison among DSDV, DSR and AODV Protocols in wireless sensor network” IEEE, International Conference on Education and e-Learning Innovations, 2012.

[7] 10 Nasrin Hakim Mithila, “Performance analysis of DSDV, AODV and DSR in Wireless Sensor Network” International Journal of Advanced Research in Computer Science and Electronics Engineering (IJARCSEE) Volume 2, Issue 4, pp.395-404, April 2013.

[8] Ipsita Panda “A Survey on Routing Protocols of MANETs by Using QoS Metrics” International Journal of Advanced Research in Computer Science and Software Engineering, Volume 2, Issue 10, pp. 121-129, 2012.

[9] C. Karlof and D. Wagner, Secure Routing in Sensor Networks: Attacks and Countermeasures, In Proc. of First IEEE International Workshop on Sensor Network Protocols and Applications, 2003.

[10] Shio Kumar Singh, M P Singh, and D K Singh“A Survey on Network Security and Attack Defense Mechanism for Wireless Sensor Networks” International Journal of Computer Trends and Technology (IJCTT) pp. 1-9, May to June 2011.

[11] 10L.L. Fernandes, “Introduction to Wireless Sensor Networks Report”, http://dit.unitn.it/~fernand/downloads/iwsn.pdf, University of Trento. 2007

[12] A. T. Zia, “A Security Framework for Wireless Sensor Networks”. 2008, http://ses.library.usyd.edu.au/bitstream/2123/2258/4/02whole.pdf.

[13] Amee A. Patel, Sunil J. Soni, “A Novel Proposal for Defending Against Vampire Attack in WSN”, IEEE Fifth International Conference on Communication Systems and Network Technologies, 2015.

[14] Chen Hongsong, Han Zhi, Fu Zhongchuan, “Quantitative Trustworthy Evaluation Scheme For Trust Routing Scheme in Wireless Sensor Networks”, IEEE Trustcom/BigDataSE/ISPA, pp. 1272-1278, 2015.

[15] Miss. Prachi, S. Moon, Mr. Piyush, K. Ingole, “An Overview on: Intrusion Detection System with Secure Hybrid Mechanism in Wireless Sensor Network” IEEE International Conference on Advances in Computer Engineering and Applications (ICACEA), pp.272-277, 2015.

[16] Lina R. Deshmukh, Prof. A. D. Potgantwar, "Ensuring an Early Recognition and Avoidance of the Vampire Attacks in WSN using Routing Loops", IEEE International Advance Computing Conference (IACC), 2015.

[17] Eugene Y. Vasserman and Nicholas Hopper “Vampire Attacks: Draining Life from Wireless Ad Hoc Sensor Networks” IEEE Transactions on Mobile Computing, Vol. 12, No. 2, February 2013.

[18] Kashif Saghar, David Kendall, Ahmed Bouridane "RAEED: A solution for Hello Flood Attack", Proceedings of 2015 12th IEEE International Bhurban Conference on Applied Sciences & Technology (IBCAST) Islamabad, Pakistan, 13th – 17th January, 2015.

[19] [Raja Waseem Anwar, Majid Bakhtiari, Anazida Zainal, Abdul Hanan Abdullah and Kashif Naseer Qureshi , “Enhanced Trust Aware Routing against Wormhole Attacks in Wireless Sensor Networks” IEEE International Conference on Smart Sensors and Application (ICSSA), 2015.