Current Trends in Technology and Science
ISSN: 2279-0535. Volume: VII, Issue: VI

Intrusion Detection System to Secure Routing Performance from Vampire Attack in WSN

Sonali Mahaver
M. Tech. Scholar Department of CSE TIT, RGPV, Bhopal M.P., India
sonalimahaver@gmail.com

Prof. Kamlesh Chandravanshi
Department of CSE TIT, RGPV, Bhopal M.P., India
kamlesh.vjti@gmail.com

Prof. Gaurav Soni
Department of CSE TIT, RGPV, Bhopal M.P., India
gauravsoni.rits@gmail.com

Abstract— *The nodes in WSN are energy constrained since nodes operate with limited battery energy. If some nodes die early due to lack of energy, they cannot communicate with each other. The presence of Vampire attacker in network is consumes the sensor nodes resources like energy and bandwidth. In this dissertation the proposed IDS security scheme is detect and prevent vampire routing in WSN. Security is required in WSN because attacker is consuming the useful energy of nodes i.e. necessary for communication in network. The normal performance of WSN is very well known and unusual performance of network is identified by proposed IDS. The comparison of existing base work and Proposed IDS is identified the network abnormal conditions in presence of abnormal conditions. The IDS is also checking the status of energy consumption with respect of successful data receiving and routing packets flooding in network. The energy utilization is better in presence of existing scheme and proposed IDS scheme because the packet receiving is better but due to presence of Vampire attacker. The proposed security scheme provides the better results as compare to existing scheme because the existing scheme is only detecting the attacker presence and proposed IDS is detect as well as also prevent WSN from attacker. The proposed security scheme is providing better performance and also removes flooding infection completely from sensor network.*

Keyword:- WSN, Routing, Energy, Vampire Attack, Existing work, Flooding, Security, IDS.

I. 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 sensor nodes are flexibility for communicating among nearby nodes or to sending data to 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 Wireless Sensor 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. This information is usually created accessible to the user through one or more gateway nodes [3]. The sensor is very tiny and having limited battery capacity.

Basically, the sensor nodes consist of sensing, mobilizes, processing, communication and power units (some of these components are optional like the mobilizes). 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, a vicinity, 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. 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.

II. 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 [4, 5, 6]. Routing paths can be established in one of three ways, namely proactive, reactive or hybrid.

A. 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 updating 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

B. Reactive (on-demand) Routing Protocol

The reactive routing protocols re maintaining the connection in a 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 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

C. 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) [7].

III. 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 [8, 9, 10] 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 [7].

Wormholes

Wormhole attack [8] 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 destructive attack is the Vampire 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.

A Vampire attack [11, 12] in sensor networks and networks in general is defined as any event that eliminates the network's capacity to perform its desired function. Attacker tries to exhaust the resources available to the victim node, by transmitting additional unwanted packets and thus prevent legitimate sensor network users from tapping work or resources to which these nodes are deployed. Vampire attack is means that not only for the adversary's attempt to subvert, disrupt, or destroy a sensor network, but also for any event that diminishes a sensor network's capability to provide a service. In network any node as normal node or week node in the radio range on attacker node agree with communication through attacker node by reply the request of attacker, so that probing packet receive by the attack node and infect through infection, after infection this infected node launch the Vampire attack

IV. SECURITY SCHEMES IN WSN

Security schemes are providing the free environment from malicious nodes or also protect the network from attack.

This paper [11] firstly targets to evaluate these vulnerabilities to routing layer battery reduction attacks. Secondly it focuses upon the change in an existing routing protocol to bound loss due to Vampire attacks at the time of forwarding of packets. Third aspect, this paper targets to surface outcomes measuring the functionality of various representative protocols in the existence of an individual Vampire. Attacker effort can be thought of attack resistant

low energy routing; in which the intruder's objective is to decrease the energy savings.

In this paper [12], proposed security against Vampire attack. vampire attack as the composition and transmission of a message that causes more energy to be consumed by the network than if an honest node transmitted a message of identical size to the same destination, although using different packet headers. We measure the strength of the attack by the ratio of network energy used in the benign case to the energy used in the malicious case, i.e., the ratio of network-wide power utilization with malicious nodes present to energy usage with only honest nodes when the number and size of packets sent remains constant. Energy use by malicious nodes is not considered, since they can always unilaterally drain their own batteries.

In this paper [13] to detect malicious data injections, we propose an algorithm that characterizes the relationships between the sensors' reported values arising from the spatial correlations present in the physical phenomenon. Even though correlation-based analyses may easily spot a single malicious measurement, the problem becomes more difficult in the presence of multiple malicious measurements, originating from colluding sensors. They define collusion as the process of injecting malicious measurements through multiple sensors in a coordinated fashion. They do not make assumptions about how colluding sensors manifest but we highlight that collusion may enable eliciting/masking an event whilst remaining undetected and/or lead to genuine sensors being considered as compromised

Towards intrusion detection in [14] introduce a lightweight scheme for detecting selective forwarding and black hole attacks in WSN. The key idea of their scheme is to make nodes monitor their neighborhood and then communicate between each other to decide if there is an intrusion taken place. The scheme is further evaluated experimentally on a real WSN deployment. This scheme benefits from the neighbors monitoring so that there is a kind of distribution that will minimize the computation load on a detection agent node. However, there will be an increase in the communication messages between nodes during the collaboration for voting that will increase the communication overhead and as a result will deplete the power of nodes quickly. It is clear that, this scheme lacks the generality that other schemes in the same category.

Intrusion detection scheme of sinkhole attack in WSN is a more specific intrusion detection scheme to detect sinkhole attack was proposed by [15]. This scheme is composed of four modules: Local Packet Monitoring Module, Local Detection Engine Module, Cooperative Detection Engine and Local Response Model. The proposed scheme has been implemented in the TinyOS environment with MinRoute protocol. A suitable detection rules have been prepared to suite with the sinkhole attack. Generally, this scheme satisfies the distribution feature of IDS which is highly required on a large scale and autonomous environment like WSN. The problem here still with the communication overhead between the nodes to exchange useful information that helps in detecting the attack.

In [16] present an intrusion detection architecture based on collaboration between neighbors. They evaluated their scheme for detecting three types of attacks: Hello flood, selective forwarding and jamming attacks. Their scheme was implemented for Collaboration Tree Protocol (CTP) on the Tiny OS environment. Although, the collaboration among nodes makes this scheme strong, the communication overhead is a problem. In addition, the extracted features that are used to construct the rules like packet sending rate and packet dropping rate caused a high false alarm for detecting attacks. Another drawback of this study is that it did not consider the power consumption rate related to the performance which is a very critical issue in WSNs.

V. Proposed Work

The unnecessary energy consumption is the intrusion of any fake communication is taking place in network and with respect to energy consumption data packets receiving is really low and also the link is not break but overhead is really high. Each sensor node has limited resources of power, memory, processing and communication capabilities and functions in unattended manner. All sensor nodes sense the send sensed data periodically deliver by hop to hop manner towards the receiver using the same radio channel. In this research we develop an IDS security scheme for protecting network from Vampire Attack. The attack information is networking the unwanted delivery of data and this information in network is identified by IDS node, which works on the basis of information or behaviour injected by Vampire attacker in network. That historic analysis base detection and future time real time protection provide strength to the communication network in the form of security issue. The attacker information in network already available in attacker malicious module and IDS is recognized the attacker by their infection of unwanted packets. The number of nodes that accept the flooding data is not able to communicate with other. The proposed IDS is providing the security by disable attacker presence and provides secure communication.

Step analysis trace for detection
// check reliability on the basis of simulation data
If (data = = unwanted message && rate >= normal)
{
Packet is Vampire attack type
Infection exists in network
packet dropping is more in network
}
Step: Call protector IDS
While (IDS-Check vulnerable node && total packet receives && energy_Consuption && Packets_receiving)
{
If (Packets flooding = high && energy_consuption= high)
If (Load Limit & Energy_Consumption = = high)
{
Estimate packets flooding according to attacker
If (control rate = true) // no attacker existence
{
Packets receiving = high
Energy consumption= Normal // But less than attacker
}
Else
{

Capture Abnormal Routing details like (abnormal_pkt_type,)
Block the sender node //attacker is exist in network
Disable attacker's communication
No node in network is communicate with attacker or attacker is also not communicate }
else
{
Network is normal and communication is proper
}
}
}

In network more than one intermediate node are participating in routing. In every communication procedure the energy of mobile nodes is consumed. The senders are sending and receiving packets sensor nodes energy are consuming. In sensing and idle mode energy is also consuming. The functioning of all sensor nodes is dependent on the sensor nodes energy.

The attacker is the intermediate nodes which is not accept packets it is only flooded. These packets are not utilized for any purpose in network. The quantity of these packet is large in quantity and these packets gradually busy all intermediate nodes or receiver nodes to busy for receiving packets of attacker in WSN. All the sensor nodes are only work for malicious nodes and malicious nodes are enhancing the quantity of flooding according to time instance.

VI. Result Description

The vampire attacker is degrading the network performance and the existing work or base paper work is stop malicious activities of attacker but proposed scheme is more reliable in term of performance. The performance comparison is mentioned below: -

A. Percentage of Loss Analysis

The attacker presence is very harmful in decentralized network because attacker identification is not easy and in mobile network it is also enhance the problem of attacker presence. The number of nodes in network is flooded large amount of data packets and these packets are consuming network limited energy resource. the vampire attacker aim is only to consume all communication resources. In this graph the attacker percentage loss is measured in given simulation time of 100 seconds. The loss of percentage is reaches up to about 55%. That means due to presence of attacker about 55% of data loss but after applying IDS scheme the attacker infection in controlled in sensor network and also the performance is improves.

B. Control Packets Overhead Analysis

The packets flooding in wireless network is required to find the destination and also in mobile sensors the flooding is must require. The packets flooding is scattering in network up to destination is not found. In this analysis the packets flooding analysis is measured in existing base paper scenario, in presence of vampire attack and in presence of proposed IDS security scheme in WSN. Here due to attacker flooding the quantity of flooding packets are beyond the estimation and because of that the particular attacker recognized by IDS security system and then minimizes the overhead in WSN. The attacker presence is activated in network in simulation time of 85 seconds and after that whole network resources are consumed but after applying existing security and proposed IDS network performance are better.

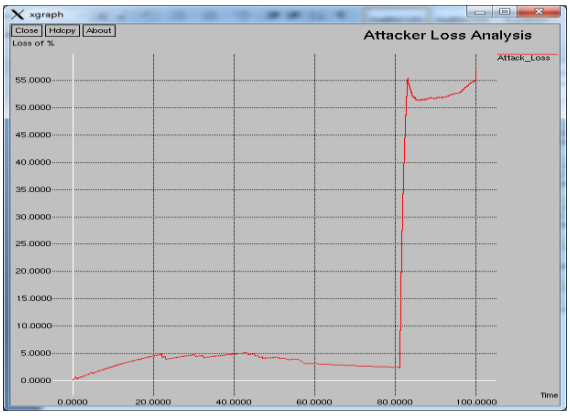

Fig.1 Attacker Loss Analysis

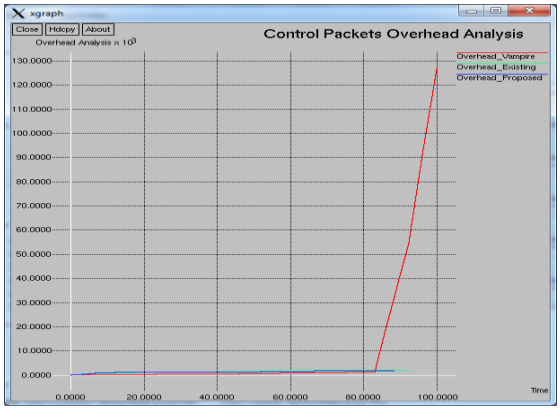

Fig.2 Overhead Analysis

Table 1 Overall Performance Analyses

Performance Metrics	Existing	Vampire Attack	Proposed IDS
Send	3723	1112	5595
Receive	3361	282	5269
Routing Packets	2115	126978	1737
Vampire Attack Pkts	6	597140	0
PDF	90.28	25.36	94.17
NRL	0.63	450.28	0.33
No. of dropped data (packets)	362	830	326

C. Summarized Network Performance Analysis

The summarized performance of Existing security scheme, Vampire Attack and proposed IDS is mentioned in table 1. The proposed security scheme is providing better results and also gives better performance of Sensor network. The number of packets sending receiving and loss and other metrics like PDF, NRL and routing packets flooding is counted up to end of simulation time. The attacker infected packets are counted in existing scheme but in proposed

scheme counting is zero that shows the better IDS performance.

VII. Conclusion and Future Work

The sensors are independent in network without any presence of Base Station or organization. In this research work we work on security against vampire attack in network. The proposed IDS algorithm is detecting Vampire attacker and identified the routing misbehaviour in network. The working of nodes is battery power or energy dependent having limited lifetime and this energy is consumed by attacker unnecessary in network. In attacker presence the packet receiving in network is minimizes but the energy consumption according to packet receiving is more. The flooding of packets is showing the abnormal behaviour of network conditions. The performance of proposed scheme is providing the better performance of existing routing scheme in WSN. The existing scheme is showing the negligible infection but in proposed IDS injecting of unwanted packets are negligible and packets receiving is also improves. The energy utilization in both existing scheme and proposed scheme is better as compare to attacker module. The performance metrics are showing the better results in presence of proposed IDS scheme. The unnecessary flooding is removes by that energy utilization and bandwidth utilization is provides better performance and also better performance reduces the packet dropping. In future we tend to implement proposed IDS in Internet of Things (IoT) in wireless network. The sensors are controlled the other sensors and attacker are also controlled network sensor nodes. In future we work on celebrative attack like Vampire attack and blackhole attack in network and measure combined malicious performance and also implement new IDS scheme for that combined attacker malicious effect in IoT devices in WSN.

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] Clement 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.

[5] 4 9 Faleh 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.

[6] 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.

[7] 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.

[8] 5.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.

[9] 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.

[10] 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, 2010, pp. 14-27.

[11] 15 Prof. A. D. Potgantwar, Lina R. Deshmukh, "Ensuring an Early Recognition and Avoidance of the Vampire Attacks in WSN using Routing Loops", IEEE International Advance Computing Conference (IACC), 2015.

[12] 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.

[13] Vittorio P. Illiano and Emil C. Lupu, "Detecting Malicious Data Injections in Event Detection Wireless Sensor Networks", IEEE Transactions on Network and Service Management, Vol. 12, No. 3, September 2015.

[14] Krontiris, I., T. Dimitriou and F.C. Freiling, "Towards Intrusion Detection In Wireless Sensor Networks", Proceeding of the 13th European Wireless Conference, CiteSeer, 2007.

[15] Krontiris, I., T. Dimitriou, T. Giannetsos and M. Mpasoukos, "Intrusion Detection Of Sinkhole Attacks In Wireless Sensor Networks" Proceedings of the 3rd International Conference on Algorithmic Aspects of Wireless Sensor Networks, (AAWSN’ 28), Springer-Verlag Berlin, Heidelberg, pp: 150- 161, 2008.

[16] Lemos, M.V.D.S., L.B. Leal and R.H. Filho, "A New Collaborative Approach for Intrusion Detection System on Wireless Sensor Networks", Novel Algorithms Techniques Telecommunication Network, pp. 239-244, 2010.