ISSN 2395-1621

ANALYTICAL REPRESENTATION OF IDENTITY DECEPTION ATTACKS OVER DATA AGGREGATION

[#1]Jyoti Rajgade, [#2]Prof. Santhosh Waghmode

[1]jsrajgade@gmail.com
[2]stwaghmode@gmail.com

[#12]Department of Computer Engineering

Imperial College of Engineering and Research,
Wagholi, Pune.

ABSTRACT

Wireless Sensor Networks came into prominence around the start of this millennium motivated by the omnipresent scenario of small-sized sensors with limited power deployed in large numbers over an area to monitor different phenomenon. The sole motivation of a large portion of research efforts has been to maximize the lifetime of the network, where network lifetime is typically measured from the instant of deployment to the point when one of the nodes has expended its limited power source and becomes in operational commonly referred as first node failure. In Wireless sensor network power and energy resources are limited. The number of sensor nodes can detect simultaneously a single target of interest. If every node sends data to the base station, energy will be wasted and thus the network energy will be consume quickly. However such aggregation is known to be highly vulnerable to node compromising attacks. Thus, ascertaining trustworthiness of data and reputation of sensor nodes is crucial for WSN. Considering the role of wireless adversary, which targets the packets of high importance by emitting radio frequency signals and do not follow underlying network architecture. Typically, jamming attacks have been considered under external threat model, in which jammer is the part of network. here proposed the new attack on WSN, carousel attack and stretch attack during the packet forwarding source to destination and discuss countermeasures that can be used to defend against these attacks.

ARTICLE INFO

Article History

Received: 5th August 2017

Received in revised form :

5th August 2017

Accepted: 11th August 2017

Published online :

19th August 2017

Keyword: Vampire attack, wireless sensor network, DOS, Security.

I. INTRODUCTION

Wireless technologies have become increasingly popular in our everyday business and personal lives. It enables one or more devices to communicate without physical connections without requiring network or peripheral cabling. As we know that wireless networks serve as the transport mechanism between devices and among devices. However, because of this wireless nature these are prone to multiple security threats in which one of the major serious security threat is jamming. Jamming can disrupt wireless transmission and can occur either unintentionally in the form of noise or interference at the receiver side. Wireless sensor networks provide efficient and reliable observation of some features of physical phenomena which are otherwise very difficult to observe and also the initiation of right actions based on collective in-formation from sensor nodes. This feature of WSN has a significant impact on several military and civil applications such as target tracking, disaster management, field surveillance, environmental and habitat monitoring, health care application, home automation and traffic control. As the application areas of wireless sensor networks continue to grow, security becomes important. Vampire attacks are not protocol specific rather uses its compliant message. Vampire attacks are caused when a message is been initiated and transmitted through a malicious node over the network causing higher battery utilization and battery exhaustion. Vampire attacks are not constrained to a specific type of protocol and does not alter specific path in the network. When a network is been attacked by them, even transfer of small data consumes more energy.

1.1 TYPES OF VAMPIRE ATTACKS

There are two type of protocols prone to vampire attacks that are identified:

- **Stateless Protocol:** In this protocol, the initial node caries the address of the direction to be followed to reach the destination node. These protocols make systems robust but are prone to attacks.
- **Stateful Protocol:** These protocols make decision for flow of data when in stored state and are also prone to attacks.

There are four different types of attacks on these two protocols.

1. Carousel attack: The stateless protocols are prone to this kind of attacks. These attacks lengthen the route and causes lesser verification of message header from where the message has to pass on.
2. Stretch attack: These attacks are also caused on a stateless protocol. These attacks stretches the number of nodes in the path and creates artificial long routes.
3. Directional Antenna Attack: The stateful protocol are prone to these attacks. This causes additional energy consumption at the source node and also consumes energy of the nodes that are not part of the path for packet transmission.
4. Malicious Discovery Attack: This attack also directs towards stateful protocol. In these attacks an error is created stating the link does not exist and a new nonexistent link is been made.

1.2 Security Requirements

The objective of security of WSNs is to provide protection for the information and resources against attacks and misuse. WSN`s security requirements are.

1.2.1 Availability
Availability ensures that the network nodes remain in stable condition and keep network services available even if attacked by denial-of-service attacks.

1.2.2 Authorization
Authorization put restriction that only authorized nodes, are allowed to be part of network and gather information for network operations.

1.2.3 Authentication
This makes sure that the information transfer from one node to another node is real, that is, a malicious node cannot act as any other network node by capturing its identity.

1.2.4 Confidentiality
Confidentiality imposes security such that a given message cannot be interpreted by any node other than the intended receiver.

1.2.5 Integrity
This ensures that a message sent from one network node to another, is not altered by malicious intermediate nodes.

1.2.6 Not Repudiation
Under this any node that sends a message to any other network node, cannot deny later on that this message has been sent by itself.

1.2.7 Freshness
Freshness of message means that the data is latest and ensures that no intruder can resend previous messages.

II. BACKGROUND STUDY

Wireless Sensor Networks are sensitive to various types of attack. They can be categorized in three types, attacks on availability of network, attacks on secrecy and authentication of network, and stealthy attack for service integrity: which makes network to allow false data value to enter in network. In these type attacks, it is important to keep network alive until desired goal of network not completes. DoS attack may cause real world harm to people`s life by affecting WSN surrounding those people. Usually DoS attack aim to destroy or disrupt a network. However, a DoS attack can be any event that declines or completely destroy capacity of network and makes it unable to conduct desired operations. There are several standard solutions present in the literature to handle with some type of denial of service attacks, although in overall, developing a common defense solution against DoS attacks is still a big issue. Some of the important attacks are briefed below:

2.1 Wormhole
A wormhole is low latency link between two portions of a network over which an attacker replays network messages .The attacker receives packets at one part of the network, and tunnels them to another part in the network, where the packets are reinitiated into the network. The tunnel among the two conspiring attackers is known as the wormhole. This link may be generated either by a single node transferring messages among two adjacent but non-neighboring nodes or by two nodes which are located in two different parts of network and having data transfer using tunnel. Radio channel used in sensors network have a broadcast feature which make attacker enable to create wormhole tunnel even for those data packets which are not addressed to it. Routing in WSN will not be possible until some efficient security methods are applied to protect network against such attacks.

2.2 Black and Gray Hole
In this attack, a attacker node falsely claims optimal paths (e.g. the shortest path or the most reliable path) to the targeted node during the route detection, or in the route updates messages. The aim of the malicious node could be to disrupt the route detection process or to capture all data packets being sent from sender to the destination node. A finer form of black hole attack is called as the gray hole attack, where the false node irregularly drops the data packets so that its detection becomes even more difficult.

2.3 Flooding
Flooding cause's memory depletion, which is very vulnerable in case where a protocol is used to maintain steady condition at any end of the connection. An attacker continuously try to make new connection request until the all sensor nodes of network consumes all the resources or

crosses their threshold limit. In any case, further true node connection requests will be ignored.

2.4 Vampire

A new class of resource depletion attack has been discovered which permanently disable network by draining energy of network nodes called "**Vampire Attack**". Vampire attacks are not affect any specific protocol. Vampire attack causes composition and flooding of messages more similar to that generated by an honest node and drains the battery life from network nodes. Basically vampire attack is a variant of DDOS attack, which performs resources consumption on neighbor nodes. Therefore during the vampire attack targeted packets are modified for preparing long routes or misguiding the packets. In addition of that the malicious nodes are making frequent connectivity from the entire neighbor nodes in network using false control message exchange. Due to these neighbor nodes replies the false request for connectivity and draining energy rapidly. On the other hand the malicious host only change a few information of the packets thus it is difficult to locate on network. Thus detecting such kind of malicious host is a complex issue.

III. LITURATURE SURVEY

Yuzhe Li, Ling Shi, Peng Cheng, Jiming Chen, and Daniel E. Quevedo presented a CPS scenario where a malicious agent carries out jamming attacks on the communication channel between a sensor and a remote estimator. he first considered a situation where the sensor and the attacker fix their strategies apriori. For the case where the sensor and the attacker have on-line information about the previous transmission outcomes and the occurrence of attacks.[1]

Eugene Y. Vasserman and Nicholas Hopper identified a single Vampire can increase network-wide energy usage by a factor of O(N), where N in the number of network nodes.They discussed methods to ease these types of attacks, considering a new proof-of-concept protocol that provably limits the damage caused by Vampire attacks during the packet forwarding phase.[3]

Sureka.N and Chandra Sekaran proposed to eliminate the advisory attack energy level constraint algorithm proficiently identifies the malicious nodes from the network, by removing those affected nodes we can transform to secure network with authenticated data transmission. The graphical result represents the enhanced network performance with increased throughput rate and improved packet delivery ratio is unbounded, indicating that the attacker can successfully destabilize the system.[4]

Saurabh Amin, Alvaro A. Cardenas, and S. Shankar Sastry, ,in this paper authors considers the network security problem constrained optimal control for discrete-time, linear dynamical systems in which control and measurement packets are transmitted over a communication network. The packets may be jammed or compromised by a malicious adversary. For a class of denial-of- service (DoS) attack models, the goal is to find an (optimal) causal feedback controller that minimizes a given objective function subject to safety and power constraints. He present a semi definite programming based solution for solving this problem.[5]

P.Rajipriyadharshini,V.Venkatakrishnan,S.Suganya,A.Masanam, in this title discuss Nowadays one main issue in wireless ad-hoc sensor network is wastage of energy at each antenna nodes. Energy is the one most important issue while considering sensor nodes. Wireless sensor networks need solution for preserve energy level. One new type of attack called vampire attack, which happening at network layer. It leads to reserve reduction(energy) at each transmitter nodes, by destroy battery power of any node. It transmit a small complaint messages to disable a whole network, hence it is very hard to detect and prevent. Existing protocol are not focus on this vampire attack occurrence on routing layer, hence there exist two types of attacks - carousel attack and stretch attack. Hence there is a large of energy loss. New protocol called PLGP, a expensive and secure protocol is planned along with the key organization protocol called Elliptic Deffi Hellman key exchange protocol to avoid this vampire attack.[7]

G. Lakshmi Narayana and Koteswara Rao discussed the Computed Energy level of the nodes. Discussed algorithm computed the influence of the attack by the ratio of network energy used in compassionate case to the energy used in the malicious case i.e. the relation of network wide power operation with malicious nodes present to energy process with only honest nodes when the number and size of packets sent remains steady and also described a new methodology based on energy threshold and packet broadcast threshold of sensor node of network. There was the dynamic detection of removal of vampire attack. This solution is simple and also works with topology change in network.[9]

IV. PROPOSED WORK

As we have studied working of vampire attacker which drains network energy by flooding packets and RREQ flooding, so that broadcast rate of vampire node will be hire and also it has hire energy than other network nodes.

Carousel Attack Module: The carousel attack is carried on wireless sensor networks shown in figure 4.1. In this type of attack a series of loop is formed between the source and the sink node. So the route length is increased and goes beyond the limit of nodes in the network. Due to this energy consumption of nodes increases and thus minimizes the network lifetime. By a factor of energy usage increases, where the maximum route length is lamda. Energy consumption during attack is measured. In first carousel attack, adversary composes packets with purposely introduced routing loops there is packet is

under loop condition. This is called as carousel attack, it sends packets in circles. This attack targets source routing protocols by exploiting the limited
verification of message headers at forwarding nodes, allowing a single packet to repeatedly traverse the same set of nodes. In this attack, an adversary sends a packet with a route composed as a series of loops, such that the same node appears in the route many times. This strategy can be used to increase the route length beyond the number of nodes in the network, only limited by the number of allowed entries in the source route. The noxious hub orchestrates bundles with intentionally presented directing circles. In light of restricted check of parcel header at sending hubs, it permits a private bundle to more than once navigate the same set of hubs. Figure shows a representation of carousel attack. Source node transmits a packet to sink. The required path is Source-E-F-Sink. But malicious node moves the packet to Source-D-C-B-A-F-Sink. In between D-C-B-A-F-E path repeated 2-3 times. The transmitted packet moves in loop for no. of times. It causes energy drain.

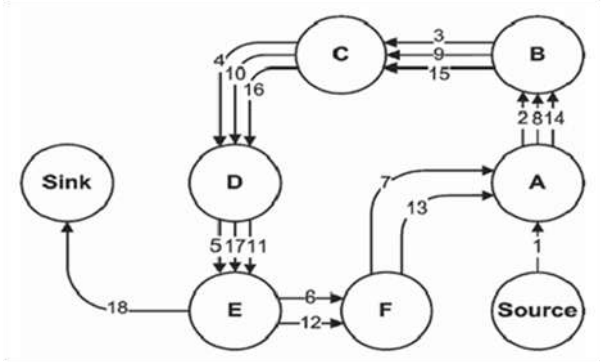


Figure 4.1: Carousel attack flow

Stretch Attack Module:
The stretch attack is carried on wireless sensor networks shown in figure 4.2. In this type of attack artificially a long route from source to sink is made by an adversary causing packets to traverse a larger route and draining extra energy. This attack causes a node that doesn't lie on optimal path to process packets. By a factor of O(min(N, lamda)), where the number of nodes in the network is N and the maximum path length is lamda. Energy consumption during attack is measured.

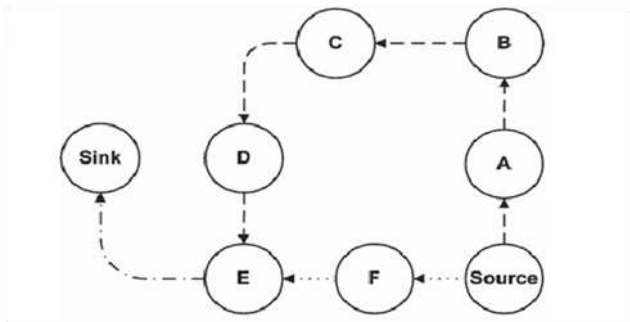
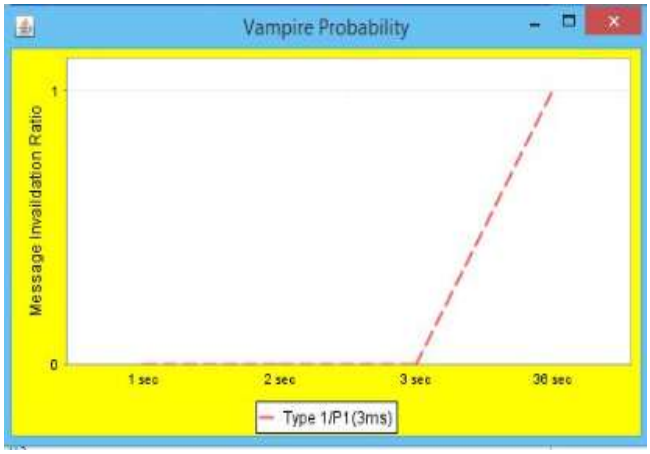
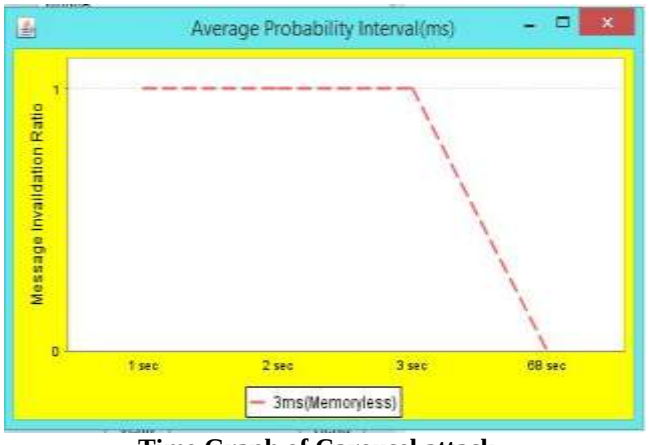


Figure 4.2: Stretch attack flow

This attack, also targeting source routing, an adversary constructs artificially long routes, potentially traversing every node in the network. This is called as stretch attack, since it increases packet path lengths, causing packets to be processed by a number of nodes that is independent of hop count along the shortest path between the adversary and packet destination. A single attacker can use a carousel attack to increase energy consumption by as much as a factor , while stretch attacks increase energy usage by up to an order of magnitude, depending on the position of the malicious node. The malicious node purposely creates long routes, probable traversing every node in the network. Figure shows stretch attack.The valid route from source to sink is source-E-F-sink, but malicious node chooses the longest route like source-D-C-B-A-F-Sink. Stretch attack is difficult to detect. Graphs of both attacks which represent time taken by both attacks are seen below as:



Time Graph of Stretch attack



Time Graph of Carousel attack

V. CONCLUSION

This work includes study of security breach of WSN by vampire attack for various stateless and state full routing protocols and different solution provided to deal with vampire attack in literature survey. Proposed methodology supposed to provide an analytical presentation of attacks which occurs in WSN. It is seen that time taken by attacks are presented graphically. In

near future a new technique according to proposed methodology is implemented using NS2 network simulator and the performance of the network under vampire network in terms of energy, PDR and throughput is provided.

REFERENCES

[1] Yuzhe Li, Ling Shi, Peng Cheng, Jiming Chen, and Daniel E. Quevedo, Jamming Attacks on Remote State Estimation in Cyber-Physical Systems: A Game-Theoretic Approach, IEEE TRANSACTIONS ON AUTOMATIC CONTROL, VOL. 60, NO. 10, OCTOBER,2015.

[2] Shyamala Ramachandran and Valli Shanmugam Detecting and preventing vampire attack in wireless sensor network proc. Sensor & Ubiquitous Computing International journal of ad-hoc, Vol.3, No.4, August 2012.

[3] Eugene Y. Vasserman and Nicholas HopperVampire Attacks: Draining Life from WirelessAd Hoc Sensor Networks IEEE Transactionson Mobile Computing, Vol. 12, No-2, 2013.

[4] Prof. S. Chandra Sekaran and Sureka.N Securable Routing And Elimination Of Adversary Attack From Manet proc. ICGICT, Vol. 2, Issue 1, 2014.

[5] Saurabh Amin, Alvaro A. Cardenas, and S. Shankar Sastry, Safe and Secure Networked Control Systems under Denial-of-Service Attacks R. Majumdar and P. Tabuada (Eds.): HSCC 2009, LNCS 5469, pp. 3145, 2009. c Springer-Verlag Berlin Heidelberg 2009.

[6] T.Sathyamorthi, D.Vijayachakaravarthy, R.Divya, M. Nandhini A Simple and Effective Scheme to find Malicious node in Wireless Sensor Network International Journal of Research in Engg. And Tech.,Vol. 3, Issue 2, 2014.

[7]P.Rajipriyadharshini,V.Venkatakrishnan,S.Suganya,A. Masanam,Vampire Attacks Deploying Resources in Wireless Sensor Networks (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 5 (3) , 2014, 2951-2953.

[8] Tran Van Phuong, Le Xuan Hung, Seong Jin Cho, Young-Koo Lee and Sung young Lee. An Anomaly Detection Algorithm for Detecting Attacks in Wireless Sensor Networks Computer Engineering Dept. Kyung Hee University 449-701 Suwon, Re- public of Korea.

[9] G.Lakshmi Narayana and Koteswara Rao,(2015), A Sensor Network Routing Protocol To Clear The Damage From Vampire Attacks During Packet Forwarding, International Journal of Science Engineering and Advance Technology, Volume 03, Issue 01.

[10] E. Ayday, H. Lee, and F. Fekri, An iterative algorithm for trust and reputation management, in Proceedings of the 2009 IEEE international conference on Symposium on Information Theory -Volume 3, ser. ISIT09, 2009, pp. 20512055.

[11] C. T. Chou, A. Ignatovic, and W. Hu, Efficient computation of robust average of compressive sensing data in wireless sensor networks in the presence of sensor faults, Parallel and Distributed Systems, IEEE Transactions on, vol. 24, no. 8, pp. 15251534, Aug 2013.

[12] Y. Yu, K. Li, W. Zhou, and P. Li, Trust mechanisms in wire-less sensor networks: Attack analysis and countermeasures, Journal of Network and Computer Applications, vol. 35, no. 3, pp. 867 880, 2012, ce:title Special Issue on Trusted Computing and Communications/ce:title.

