ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 4, April 2016

A Survey on Trivial Secure Trick for Source Imitations and Packet Drop Attacks in Wireless Sensor Networks

Namrata Bannur[1], S. R. Purohit[2], Ratna Patil[1], Shitalrani S[1], Ravindra Banakapur[1]

P.G. Student, Dept. of Electronics & Communication Engineering, BLDEA's V.P.Dr.PGH CET, Vijayapur, Karnataka, India[1]

Associate Professor, Dept. of Electronics & Communication Engineering, BLDEA's V.P.Dr.PGH CET, Vijayapur, Karnataka, India[2]

ABSTRACT: Sensor systems are conveyed for various application spaces and that information gathered by them is utilized as a part of choice making for foundations. Information are spilled from different source through halfway handling nodes that total the data .The information dependability is an imperative element as an aggressor bargains those sorts of system by presenting extra system nodes in the system or trading off the current nodes. The few testing prerequisites are low vitality and data transfer capacity utilization, proficient capacity and secure transmission. This overview depicted distinctive attacks, provenance falsification and way scuring techniques with viability and productivity to fulfill these requirements and to safeguard honesty and classification of provenance impersonation and parcel trickle attacks in WSN.

KEYWORDS: Provenance forgery attack, Bloom Filter, Data Provenance, Denial of service attacks, WSN.

I. INTRODUCTION

Remote sensor systems are most progressively utilized as a part of a few applications, for example, wild natural surroundings observing, woodland fire recognition, and military reconnaissance region. In the wake of being conveyed in the field of interest, sensor nodes arrange themselves into a multihop system range with the base station. Regularly, a sensor node is seriously obliged regarding calculation ability and vitality saves.

Sensor systems are utilized as a part of various application spaces, for example, cyber physical base frameworks, natural observing and power matrices. Information are delivered at countless node sources and prepared in system at moderate jumps system on their way to a Base Station that performs choice making [1]. The differing qualities of information sources make the need to guarantee the reliability of information, for example, just dependable data is considered in the choice procedure.

In a multi-bounces sensor system and information provenance permits the BS to follow the source and sending way of an individual information parcels. Provenance must be recorded for every bundle, except imperative difficulties emerge because of the tight stockpiling, vitality and data transmission requirement of sensor nodes. Consequently, it is important to devise a light-weight provenance arrangement with low overhead.

Thus it's important to address security prerequisites like secrecy, uprightness and freshness of provenance. Our imperative objective is to plan a provenance encoding and interpreting technique that fulfills security and execution need.

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 4, April 2016

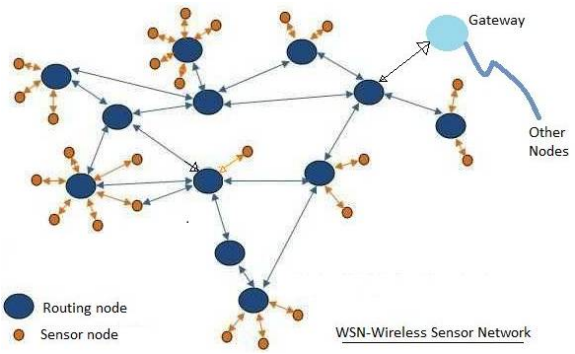

Fig 1: Typical WSN

II. DIFFERENT ATTACKS IN WSN

Here, we present some known attacks (intensively discussed in the references) that pose a significant threat to group communications over wireless networks, and categorize these attacks based on their impacts, including data integrity and confidentiality, power consumption, routing, identity, privacy, and service availability.

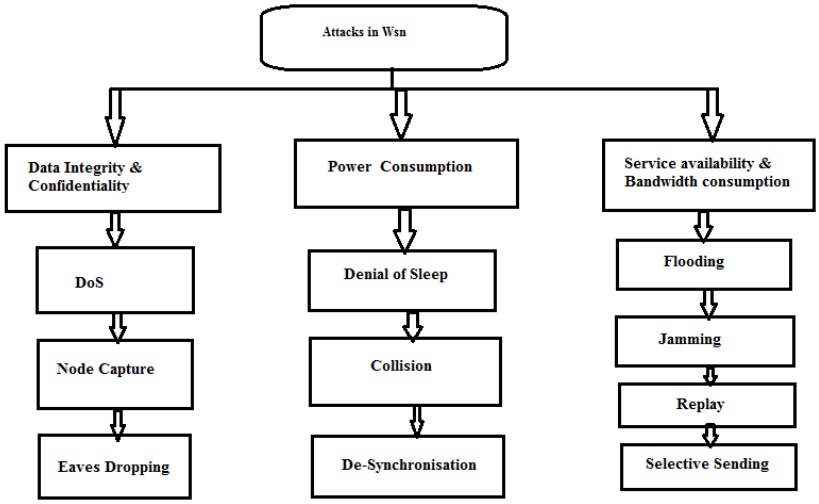

Fig 2: Different attacks in WSN

2.1 DATA INTEGRITY AND CONFIDENTIALITY-RELATED ATTACKS

In general, this type of attack attempts to reveal or compromise the integrity and confidentiality of data contained in the transmitted packets [2].

2.1.1 Denial of Service (DoS) Attack: Denial of Service attack is an attempt to make a network unavailable for its legitimate users. An attacker tampers with data before it is read by sensor nodes, thereby resulting in false readings and eventually leading to a wrong decision. A DoS attack generally targets physical layer applications in an environment where sensor nodes are located.

One common method of such attack involves saturating the target machine with external communications requests so that it cannot respond to legitimate traffic, or responds slowly. Such attacks usually lead to a server overload.

2.1.2 Node Capture Attack: In Node Capture Attack an assailant physically catches sensor nodes and bargains them so that sensor readings detected by traded off nodes are mistaken or controlled. The aggressor might likewise endeavor to concentrate fundamental cryptographic keys like a gathering key from remote nodes that are utilized to ensure correspondences in many remote systems.

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 4, April 2016

Node catch not just empowers to take a few to get back some composure of cryptographic keys and convention states, additionally to clone and redeploy noxious nodes in the system.

2.1.3 Eaves dropping attack: Eavesdropping is the procedure of get-together data from a system by snooping on transmitted information and to listen stealthily is to subtly catch a private discussion over a secret correspondence in an unapproved way. The data continues as before however its protection is traded off. An assailant listens in subtly between any two nodes and might gather the fundamental data viewing association, despite the fact that this attack can be arranged into different classifications, for example, protection related attacks, we amass it into this class since its outcomes are extreme as in the gathered cryptographic data might break the encryption keys such that the aggressor can recover significant information. An illustration of listening in is blocking charge card numbers, utilizing gadgets that intrude on remote telecast interchanges or tapping wire correspondences.

2.2 POWER CONSUMPTION RELATED ATTACKS

A standout amongst the most significant resource in remote system is the force supply. In force utilization related attacks an assailant tries to debilitate the remote gadget's energy supply and it might corrupt the lifetime of the system. A most dire outcome imaginable might even fall the system correspondence.

2.2.1 Denial of Sleep Attack: In a remote system when there is no radio transmission, the MAC layer convention decrease the node's energy utilization by directing the node's radio correspondences. An assailant might utilize this situation and attempt to deplete a remote gadget's restricted force supply (particularly sensor gadgets) so that the hub's lifetime is essentially abbreviated. In this way, the aggressor attacks the MAC layer convention to abbreviate or incapacitate the rest period. On the off chance that the quantity of force depleted nodes is sufficiently extensive, the entire sensor system can be extremely disturbed. Indeed, even with force administration instruments set up, unless a MAC convention can make chances to rest for long spans, the stage can't accomplish expanded system lifetimes.

2.2.2 Collision Attack: In this attack, aggressor tries to degenerate the octet of transmitted bundles. In the event that aggressor succeeds in doing as such; then, at the less than desirable end; the bundles will be disposed of because of checksum crisscross. The retransmission of parcels could bring about weariness of vital assets i.e. vitality of the sensor nodes.

2.2.3 De-Synchronization Attack: In de-Synchronization Attacks, assailant fashions messages between endpoints. Alteration in control banners or arrangement numbers are generally made. On the off chance that the aggressor is fortunate and got the control at right timing, then he may keep the end points from regularly trading messages as they will be, by constantly asking for retransmission of lost message. This attack prompts a vast retransmission cycle that debilitates part of vitality.

2.3 SERVICE AVAILABILITY AND BANDWIDTH CONSUMPTION RELATED ATTACKS

These attacks mean to decimate the sending capacity of sending nodes or devour pitifully accessible transfer speed; they are more probable identified with accessibility of administration and data transfer capacity utilization. These attacks can likewise be sorted as force utilization related attacks. In the event that these attacks result in a disavowal of administration to honest to goodness individuals, they can likewise be alluded to as a variation of dissent of-administration (DoS) attacks.

2.3.1 Flooding Attack: There are different sorts of disavowal of administration attacks which are arranged in various way and abatements system lifetime in various ways. One among them is the flooding sort of Denial of Service attack. An assailant utilizing this sort of attack typically sends countless to the casualty or to an entrance point to keep the casualty or the whole system from building up or proceeding with interchanges. The essential point of flooding attacks is to bring about fatigue of assets on casualty framework.

2.3.2 Jamming (Radio Interference) Attack: Jamming is one of numerous exercises used to bargain the remote environment. One of the central routes for jamming to debase the system execution is remote transmissions. An assailant can honorably remove the connection among nodes by conveying consistent radio flags so that other authorized clients are not permitted to get to a specific recurrence channel. The aggressor can likewise send sticking radio signs, which deliberately crash into, honest to goodness signals started by target nodes.

2.3.3 Replay Attack: A replay attack is a type of system attack in which a legitimate information transmission is vindictively or falsely rehashed or postponed. This is completed either by the originator or by an aggressor who blocks the information and retransmits it, perhaps as a feature of a masquerade attack by IP bundle substitution, (for example,

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 4, April 2016

stream figure attack). An aggressor duplicates a sent parcel and later conveys the duplicates over and again and ceaselessly to the casualty with a specific end goal to deplete the casualty's supports or power supplies, or to base stations and get to indicates all together corrupt system execution.

2.4.4 Selective sending attack: This attack is now and again called Gray Hole attack. In a basic type of specific sending attack, noxious nodes attempt to stop the parcels in the system by declining to forward or drop the messages going through them. There are distinctive types of specific sending attack. In one type of the specific sending attack, the malignant node can specifically drops the bundles originating from a specific nodes or a gathering of nodes. This conduct causes a DoS attack for that specific nodes or a gathering of nodes as appeared.

A sending node specifically drops bundles that have been begun or sent by specific nodes, and advances other unimportant parcels. They likewise act like a Black gap in which it declines to forward each parcel. The malignant node might forward the messages to the wrong way, making unfaithful steering data in the system.

III. SECURITY OBJECTIVES

1) Query-based frameworks: -The base station realities sink telecasts an inquiry to the system and the nodes react with the critical data. Messages from partitioned nodes are possibly collected enrooted to the base station. Finally, the base station figures one or more aggregate qualities in view of the messages it has gotten [3].

2) Event-based frameworks: - Nodes make an impression on the base station just when the objective occasion happens in the range of hobby. On the off chance that distinctive reports being spread compare to the same occasion, they can be consolidated by a middle of the road node on the course to the base station.

IMPACTS OF ATTACKS

• Confidentiality: A foe can't increase any examining so as to learn about information provenance the substance of a parcel. Just lawful gatherings (e.g., the BS) can process and check reality of provenance [4].

• Integrity: An enemy, stand-in alone or plotting with others, can't include or expel non-intriguing nodes from the provenance of favorable information produced by considerate nodes less being identified.

• Freshness: An enemy cannot replay caught information and provenance without vicinity identified by the BS.

IV. METHODS TO SECURE PROVENANCE AND PATH IN WSN

By utilizing distinctive encoding techniques, we can secure the provenance and way in WSN. Some of the strategies are

1) Cryptography
2) Cryptography with digital signature
3) Bloom filter

- **CRYPTOGRAPHY**

The word cryptography comes from the Greek words κρυπτο (hidden or secret) and γραφη (writing). Oddly enough, cryptography is the art of secret writing. More generally, people think of cryptography as the art of mangling information into apparent unintelligibility in a manner allowing a secret method of unmangling. The basic service provided by cryptography is the ability to send information between participants in a way that prevents others from reading it. The kind of cryptography is based on representing information as numbers and mathematically manipulating those numbers [5].

This kind of cryptography can provide other services, such as

• Integrity checking—reassuring the recipient of a message that the message has not been altered since it was generated by a legitimate source

• Authentication—verifying someone's (or something's) identity But back to the traditional use of cryptography.

A message in its original form is known as plaintext or clear text. The mangled information is known as cipher text. The process for producing ciphertext from plaintext is known as encryption. The reverse of encryption is called decryption. While cryptographers invent clever secret codes, cryptanalysts attempt to break these codes. These two disciplines constantly try to keep ahead of each other. Ultimately, the success of the cryptographers rests on the plaintext cipher text plaintext encryption decryption. Cryptographic systems tend to involve both an algorithm and a

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 4, April 2016

secret value. The secret value is known as the key. The reason for having a key in addition to an algorithm is that it is difficult to keep devising new algorithms that will allow reversible scrambling of information, and it is difficult to quickly explain a newly devised algorithm to the person with whom you'd like to start communicating securely.
Cryptography is the art and science of making a cryptosystem that is capable of providing information security. Cryptography deals with the actual securing of digital data. It refers to the design of mechanisms based on mathematical algorithms that provide fundamental information security services.

- **CRYPTOGRAPHY WITH DIGITAL SIGNATURE**

A major benefit of public key cryptography is that it provides a method for employing digital signatures. Digital signatures enable the recipient of the information to verify the authenticity of the information's origin, and also verify that the information is intact. Thus, digital signatures provide authentication and data integrity. A digital signature also provides non-repudiation, which means that it prevents the sender from claiming that he or she did not actually send the information. These features are every bit as fundamental to cryptography as privacy, if not more.
A digital signature serves the same purpose as a handwritten signature. However, a handwritten signature is easy to counterfeit. A digital signature is superior to a handwritten signature in that it is nearly impossible to counterfeit, and it attests to the contents of the information as well as the identity of the signer.

- **BLOOM FILTER**

A Bloom filter is a space-efficient probabilistic data structure, conceived by Burton Howard Bloom in 1970, that is used to test whether an element is a member of a set. False positive matches are possible, but false negatives are not, thus a Bloom filter has a 100% recall rate. In other words, a query returns either "possibly in set" or "definitely not in set".
Elements can be added to the set, but not removed (though this can be addressed with a "counting" filter). The more elements that are added to the set, the larger the probability of false positives.

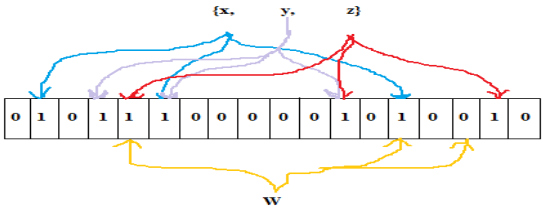

Fig 3: An Example of Bloom filter

An example of a Bloom filter, representing the set {*x*, *y*, *z* }. The colored arrows show the positions in the bit array that each set element is mapped to. The element *w* is not in the set {*x*, *y*, *z*}, because it hashes to one bit-array position containing 0. For this figure, $m = 18$ and $k = 3$. Bloom filters also have the unusual property that the time needed either to add items or to check whether an item is in the set is a fixed constant, O(*k*), completely independent of the number of items already in the set. No other constant-space set data structure has this property, but the average access time of sparse hash tables can make them faster in practice than some Bloom filters.

V. CONCLUSION

In this paper, the threats and vulnerabilities to WSNs are identified and the various categories of such attacks are summarized. These threats could even prone to collapse the entire systems and networks, hence adding security in a resource constrained wireless sensor network with minimum overhead provides significant challenges, and is an ongoing area of research. The issue of safely transmitting provenance for sensor networks is considered. Proposed lightweight provenance provides encoding in view of cryptography, cryptography with digital signature and Bloom filters. This guarantees confidentiality, respectability and freshness of provenance.

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 4, April 2016

REFERENCES

1) Salmin Sultana, Gabriel Ghinita, Member, IEEE , Elisa Bertino, Fellow, IEEE , and Mohamed Shehab, Member, IEEE Computer Society, "A Lightweight Secure Scheme for Detecting Provenance Forgery and Packet Drop Attacks in Wireless Sensor Networks", IEEE TRANSACTIONS ON DEPENDABLE AND SECURE COMPUTING, VOL. 12, NO. 3, MAY/JUNE 2015.

2) K.Venkatraman, J.Vijay Daniel, G.Murugaboopathi," Various Attacks In Wireless Sensor Network" (IJSCE) ISSN: 2231-2307, Volume-3, Issue-1,page no208 March 2013.

3) Meghraj Kadam, Sagar Dakhore, Keshav Chavan, Amol Bandgar," Secure Model For Detecting Origin Forgery And Packet Drop Attacks In WSN",Mjret, *Volume 2, Issue 4,page no 823,april 2015*.

4) Ms. M. Tharani PG Scholar,"An Efficient Detection of Forgery And Packet Drop Attacks In Wireless Sensor Networks" IJAICT Volume 2, Issue 7, page no 1055,November 2015.

5) Wikipedia, www.google.com,etc.