Explore the Packet Loss due to packet Drop Attacks in Wireless Sensor Network

*Sugunasri Singidi¹, D. Vijayakumari²

#1 M.Tech Scholar (CSE) and Department of Computer Science Engineering, Kakinada Institute of Engineering and Technology for Women, Korangi, AP, India.

Abstract:
The major deputation of wireless sensor network is the effective congregating and transmission of sensed data to a base station for propel handling. The life of such a sensor system is the time amid which it can assemble data from every one of the sensors to the base station. A key test in data gathering is to expand the system lifetime, given the vitality requirements. As sensor networks are as a rule all the time more conveyed in basic leadership the procedure that on in parcel Bloom channels to encode provenance of the data. This proposed work presents effective apparatuses for provenance confirmation technique and remaking strategy at the base station with the usefulness to identify bundle drop assaults or by noxious data sending nodes. To propose a novel lightweight scheme to securely transmit provenance for sensor data. What's more the secure provenance scheme usefulness used to recognize bundle drop assaults sorted out by malignant data sending nodes. This work depicts the viability and proficiency of the Light weight secure provenance scheme in recognizing bundle fabrication and parcel misfortune assaults.

Keywords:-Wireless Sensor Networks, Attacks, Security, AODV, Throughput, Packet loss, Delay.

I. Introduction

Wireless sensor networks are most progressively utilized as a part of a few applications, for example, wild natural environments detecting, forest fire discovery, and military surveillance region. In the wake of being conveyed in the field of intrigue, sensor nodes arrange themselves into a multihop network territory with the base station. Ordinarily, a sensor node is seriously compelled as far as calculation capacity and vitality saves. Sensor networks are utilized as a part of various application spaces, for example, digital physical foundation systems, natural checking and power lattices. Data are created at an extensive number of sensor node sources and prepared in network at middle of the road jumps network on their way to a Base Station that performs basic leadership. The decent variety of data sources make the need to guarantee the reliability of data, for example, just dependable data is considered in the choice procedure. In a multi-jumps sensor network and data provenance enables the BS to follow the source and sending way of individual data parcels.

Provenance must be recorded for every parcel, except vital difficulties emerge because of the tight stockpiling, vitality and transmission capacity requirement of sensor nodes. Accordingly, it is important to devise a light-weight provenance arrangement with low overhead. Subsequently it's important to address security necessities like secrecy, uprightness and freshness of provenance. Our vital objective is to plan a provenance encoding and deciphering technique that fulfills security and execution require. We propose a provenance encoding technique whereby every node on the way of an data bundle securely installs provenance data inside a Bloom channel that is transmitted alongside the data. After accepting the parcel, the Base station extricates and confirms the provenance data. We likewise devise an augmentation of the provenance encoding scheme that enables the Base station to distinguish if a bundle drop assault was arranged by a noxious node.

II. Related work
Hyo-Sang Lim, Yang-Sae Moon and Elisa Bertino[4] propose the approach that uses the data provenance and also their qualities in creating trust scores, that is, quantitative measures of dependability. It get the trust scores, it proposes a cyclic system which well mirrors the between reliance property. The trust score of the network nodes is influenced by that made and refreshed node, and vice versa. The trust scores of data things are produced from their esteem likeness and provenance comparability. The esteem closeness is given by the rule that "the farthest homogeneous qualities, the higher the trust scores, for a similar occasion". The provenance comparability is characterized on the rule that "the higher the trust scores, the most extraordinary data provenances with comparable qualities". The primary imperfection is that this technique and multi-characteristics in-network tasks and is various ward traits are not managed and other likelihood disseminations rather than typical dispersions are not thought about [4]. The plan and execution of ExSPAN [10], that proficient network provenance is accomplished by a nonexclusive structure in a disseminated situation. To "clarify" the presence of any network state it uses the database thought of data provenance, with the end goal that a versatile activity is given by a network provenance. That adaptability can be proficient at Internet. ExSPAN utilizes the revelatory networking in persistent questions over disseminated streams are demonstrated and will be done and pronounced briefly in a definitive inquiry dialect. The provenance to empower appropriation at Internet has been created in database that has expanded existing data models, various streamlining strategies are investigated to inquiry disseminated network provenance and oversee and productively. The ExSPAN model is created utilizing Rapid Net, is utilized as a part of networking stage based on the developing ns-3 toolbox. The primary downside is does not give privacy and validness of provenance data [10]. The real security danger to the data movement is malevolent parcel [1] dropping assault in the sensor network, since it might hinder the lawful engendering of touchy data and reductions network throughput. Managing this assault is trying since the temperamental wireless correspondence. Particular highlights and resource limitations of the sensor network may deceive to some wrong determination and cause correspondence catastrophe about the nearness of such assault. This technique utilizes an instrument based on data provenance to recognize the assault; the source of the assault is distinguished notwithstanding that, i.e. the malevolent node. For this reason, the qualities of the watermarking based provenance have been used after the provenance inserting and furthermore rely upon the between parcel timing attributes. The scheme comprises of three stages (I) Detection of Packet Loss (ii) Identification of Attack Presence (iii) Localization the Malicious Node/Link. Based on the dispersion of the between parcel confine the end of bundle will be found. By contrasting the observational normal bundle misfortune rate with the characteristic parcel misfortune rate of the data stream way the nearness of the assault is resolved. The more provenance data is transmitted alongside the sensor data to confine the malignant connection. In the event that the watched conduct, purportedly of a particular client, and the learnt example of this current client's past data does not coordinate at that point Masquerade assault [1] will be accounted for. The real restriction in this procedure is that the client may authentically go astray briefly from the past conduct. In the event that the erraticism is enormous and close perpetual, at that point it is attractive that such deviations are caught in an identification instrument. This part of client conduct while recognizing masquerade assaults is additionally mulled over in this strategy. The proposed scheme is based on the commence that the orders that have been utilized by a true blue client or an aggressor and the prepared mark may contrast. In any case, the deviation of an assailant holds on longer while that of the deviation of the true blue client is fleeting. The current system doesn't appropriately address the provenance in sensor networks. Provenance must be recorded for every bundle, because of the transfer speed limitations, vitality and tight stockpiling, and of sensor nodes essential difficulties may emerge. For every client disguise discovery manufactures a profile by social affair data, for example, area, login time, session span, CPU time, orders issued, client ID and client IP address. At that point, these profiles against logs and flags are analyzed as an assault any conduct that does not coordinate the profile.

### III. Threat Attacks in Wireless Sensor Network

Why is security necessary in WSN? Due to the broadcast nature of the transmission medium wireless sensor networks are vulnerable. There are another reason of vulnerability of WSNs are nodes are often placed in a hostile or dangerous environment and they
are not physically safe. Most of the threats and attacks against security in wireless sensor networks are almost similar to their wired counterparts while some are exacerbated with the inclusion of wireless connectivity. WSNs are usually more vulnerable to various security threats because the unguided transmission medium is more susceptible to security attacks, but also through traffic analysis, privacy isolation, physical attacks and so on. Different possible attacks can be categorized as follows:

A. Denial of Service Attacks

In WSN, Denial of Service (DOS) is produced by the unintentional failure of nodes or malicious action. In DOS attack the adversary attempts to subvert, disrupt or destroy a network. DOS attack diminishes a network capability to provide a service for any event. The simplest DOS attack tries to exhaust the resources available to the victim node, by sending extra unnecessary packets and thus prevent legitimate network users from accessing services or resources to which they are entitled.

B. Flooding

Flooding is a DOS attack in transport layer. A protocol becomes vulnerable to memory exhaustion through flooding when it maintains at either end of a connection. An attacker may repeatedly make new connection requests until the resources required by each connection are exhausted or reach a maximum limit. In either case, further legitimate requests will be ignored. Disrupt communication is one of purpose of this attack. It creates resource exhaustion and reduces availability.

C. Black hole Attack

A malicious node acts as a black hole in the range of the sink attracts the entire traffic to be routed through it by advertising itself as the shortest route. The adversary drops packets coming from specific sources in the network. Once the malicious device is in between the communicating nodes (for example, sink and sensor node), it is able to do anything with the packets passing between them. This attack can also affect the nodes those are considerably far from the base stations. It creates high rate of packet loss, network partition. It decreases the throughput of a subset of nodes. The network architecture of this attack is traditional wireless sensor network.

D. Physical Attacks

Sensors networks typically operate in hostile outdoor environments. The sensor networks are highly susceptible to physical attacks, i.e. threats due to physical node destructions as sensors are small in size, deployed with the unattended environment. Physical attack destroys sensors permanently, so there are losses of cryptographic secrets, tamper with the associated circuitry, modify or replace sensors with malicious sensors under control of the attacker.

IV. Methodology

A. Cryptography

Cryptography is the practice and study of techniques for secure communication in the presence of third parties. More generally, it is about constructing and analyzing protocols that overcome the influence of adversaries and which are related to various aspects in information security such as data confidentiality, data integrity, authentication, and non-repudiation. Modern cryptography intersects the disciplines of mathematics, computer science, and electrical engineering. Applications of cryptography include ATM cards, computer passwords, and electronic commerce.

1. Key generation

RSA involves a public key and a private key. The public key can be known to everyone and is used for encrypting messages. Messages encrypted with the public key can only be decrypted using the private key.

2. Encryption

Alice transmits her public key \((n, e)\) to Bob and keeps the private key secret. Bob then wishes to send message \(M\) to Alice.

Alice first turns \(M\) into an integer \(m\), such that \(0 \leq m < n\) by using an agreed-upon reversible protocol known as a padding scheme. He then computes the ciphertext

\[
C = m^e \pmod{n}
\]

corresponding to.

This can be done quickly using the method of exponentiation by squaring. Bob then transmits to Alice.
Note that at least nine values of $m$ could yield a ciphertext $c$ equal to $m$, but this is very unlikely to occur in practice.

3. Decryption

Alice can recover $m$ from $c$ by using her private key exponent $M$ via computing $m = c^d \pmod{n}$. Given, she can recover the original message $M$ by reversing the padding scheme.

Provenance Module

In sign module the accompanying procedures are performed. 1. Key age, 2. encryption, 3. key trading 4. signature 5. send to confirm module

Provenance Verification

In provenance confirm module the accompanying procedures are performed. 1. Key age, 2. decryption, 3. key trading 4. send to recipient module

Provenance Collection

In the event that recipient modules gets a parcel information suspicious, it is set in suspicious box, assume if information is right it is put in region box.

Information provenance

Setup: the information maker sets up its marking key $k$ and information buyer sets up its check enter $k_0$ in a safe design that keeps malware from getting to the mystery keys.

Sign(D, $k$): the information maker signs its information D with a mystery key $k$, and yields D alongside its confirmation sig.

Confirm (sig, D, $k_0$): the information buyer utilizes key $k_0$ to check the mark sig of got information D to guarantee its source, and rejects the information if the confirmation comes up short.

B. Secure Provenance Encoding

This technique propose an appropriated component to encode provenance at the hubs and concentrated calculation to translate it at the BS. The specialized center of our proposition is the thought of in parcel Bloom channel. Every parcel comprises of an exceptional succession number, information esteem, and an iBF which holds the provenance. This paper underscore that our emphasis is on safely transmitting provenance to the BS. In a collection framework, securing the information esteems is additionally an imperative perspective, however that has been as of now tended to in past work. Our protected provenance procedure can be utilized as a part of conjunction with such work to acquire an entire arrangement that gives security to information, provenance and information provenance official.

C. Distinguishing Packet Drop Attacks

The protected provenance encoding plan to recognize bundle drop assaults and to distinguish malevolent node(s). To accept the connections on the way show regular parcel misfortune and a few ill-disposed hubs may exist on the way. For straightforwardness, this technique consider just direct information stream ways. Additionally, it don't address the issue of recuperation, once a noxious hub is recognized. Existing systems that are symmetrical to our location plan can be utilized, which may start multipath steering or fabricate a scattering tree around the traded off hubs. The expand provenance encoding to utilize a parcel affirmation that requires the sensors to transmit more meta-information.

For an information bundle, the provenance record created by a hub will now comprise of the hub ID and an affirmation as a succession number of the in conclusion observed (prepared/sent) parcel having a place with that information stream. On the off chance that there is a transitional bundle drop, a few hubs on the way don't get the parcel. Henceforth, amid the following round of parcel transmission, there will be a confuse between the affirmations created from various hubs on the way. This reality is used to distinguish the parcel drop assault and to restrict the noxious hub.

V. Secure Provenance Encoding

A disseminated component to encode provenance at the hubs and a brought together calculation to disentangle it at the BS is proposed. The specialized center of our proposition is the idea of in-bundle Bloom channel (iBF). Every bundle comprises of a kind succession number, information esteem, and an iBF which holds the provenance. In a conglomeration framework, securing the information esteems is likewise an essential viewpoint, yet that has been now tended to in past work. Our protected provenance procedure gives security to information, provenance and information provenance official.
A. PROVENANCE ENCODING

For an information parcel, provenance encoding alludes to creating the vertices in the provenance diagram and embed them into iBF. Every vertex at a hub in the information way and speaks to the provenance record of the host hub. A vertex is extraordinarily distinguished by the Vertex ID (VID). The VID is ascertained per packet in view of the parcel arrangement number (seq) and the mystery key $K_i$ of the host hub. We utilize a square figure capacity to deliver this VID in a protected way. In this way for a given information parcel, the VID of the hub $n_i$ is registered as $v_i = \text{generateVID}(n_i, \text{seq}) = E_{K_i}(\text{seq})$ (1) where $E$ is a safe square figure, for example, AES, and so on. At the point when a source hub makes a parcel, it likewise makes a BF (alluded to as ibf0), introduced to 0. The source at that point produces a vertex as indicated by Eq. (1), embeds the VID into ibf0 and transmits the BF. Upon getting parcel, each middle of the road hub $n_j$ performs information and also provenance total. On the off chance that $n_j$ gets information from a solitary youngster $n_j-1$, it totals fractional provenance contained in the bundle with its own particular provenance record. For this situation, the iBF $ibf_{j-1}$ having a place with the got parcel speaks to a halfway provenance, i.e., the provenance diagram of the sub-way from the source up to $n_j-1$. Then again, if $n_j$ has in excess of one kid, it creates an accumulated provenance from its own particular provenance record and the halfway provenance got from its kid hubs. At to start with, $n_j$ processes a BF ibf$_j$–1 by bitwise-ORing the iBFs from its kids. ibf$_j$–1 speaks to an incomplete totaled provenance from every one of the youngsters. In either case, a definitive totaled provenance is created by encoding the provenance record of $n_j$ into ibf$_j$–1.

B. PROVENANCE DECODING

At the point when the BS gathers an information bundle, it executes the provenance confirmation process, which realizes that the BS recognizes what the information way ought to be, and checks the iBF to see whether the right way it has voyage. Nonetheless, after system arrangement, and when the topology changes (e.g., because of hub disappointment), the way of a parcel sent by a source may not be known to BS. A provenance gathering process is important, which recoups provenance from the got iBF and the BS takes in the information way from a source hub. Thereafter, after social event a parcel, it is adequate for BS to confirm its provenance learning with that encoded in the bundle. Beneath we examine these procedures in detail:

Algorithm 1 Provenance Verification

Info: Received parcel with arrangement seq and iBF ibf

Set of hash capacities $H$, Data way $P = <n_1, ..., n_1, ..., n_p>$

BF$_c$ ← 0 //Initialize Bloom Filter for every $n_i$ P do

$vid_i = \text{generateVID }(n_i, \text{seq})$

insert $vid_i$ into BF$_c$ utilizing hash works in $H$

endfor

on the off chance that (BF$_c = \text{ibf}$ ) then return genuine//Provenance is checked end if

return false

Provenance Verification: The BS handles the confirmation procedure to check its provenance learning and furthermore to check the honesty of the transmitted provenance. Calculation 1 demonstrates the means to confirm provenance for the given information. We expect the learning of the BS about this information way is $P$. At in the first place, the BS introduces a Bloom channel BF$_c$ with every one of the 0’s. The BF is then refreshed by creating the VID for every hub in the way $P$ and embeddings this ID into the BF.BF now mirrors the view of BS about the encoded provenance. To approve its discernment, the BS at that point looks at BF$_c$ to the got iBF ibf . The provenance check succeeds just if BF$_c$ is equivalent to ibf . Something else, if BF$_c$ contrasts from the got iBF, it shows either an adjustment in the information stream way or a change assault in the BF. The disappointment of check triggers the provenance accumulation process which endeavors to recover the hubs from the encoded provenance and furthermore to recognize the occasions of a way change and an assault.

Provenance Collection: As clarified in the Algorithm 2, the provenance accumulation plot creates a rundown
of potential vertices in the provenance chart through the ibf enrollment testing over every one of the hubs. For every hub ni the BS makes the comparing vertex (i.e. vi with VIDvidi) utilizing Eqn. (1). The BS at that point plays out the participation question of vid inside ibf. In the event that the calculation returns genuine, the vertex is likely present in the provenance, i.e., the host hub ni is in the information way. Such a derivation may present mistakes on account of false positives (a hub not on the course is induced to be on the course). Once the BS concludes the arrangement of potential hopeful hubs S = < n1, ..., n1, n2, ..., np>, it executes the provenance confirmation calculation on this set. This progression is required to recognize the instances of a true blue course change and that of malevolent action. On the off chance that the check succeeds, we can decide the way effectively.

VI. Proposed Method

The objective is to plan a provenance encoding and interpreting instrument which fulfills security and execution needs. It proposes a provenance encoding methodology in that every hub on the way of an information bundle safely installs provenance data inside a Bloom channel (BF) ought to be transmitted alongside the information. While accepting the bundle the Base Station removes and checks the provenance data. The augmentation of the provenance encoding plan enables the BS to identify bundle drop assault composed by a malevolent hub. The highlights are:

- Formulate the issue of secure provenance transmission in sensor arranges, and recognize the difficulties particular to this unique circumstance.

- Design a successful system for provenance disentangling and confirmation at the base station.

- Extend the protected provenance encoding plan and devise a system that identifies bundle drop assaults arranged by noxious sending sensor hubs.

- Perform a definite security investigation and execution assessment of the proposed provenance encoding plan and parcel misfortune identification component.

VII. 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.

References


Authors

Sugunasri Singidi is pursuing M.Tech(CSE), in the department of CSE from Kakinada Institute of Engineering and Technology for Women, Korangi.

D. Vijayakumari is working as an Assistant Professor in Department of C.S.E, Kakinada Institute of Engineering and Technology (KIET-W), korangi, Kakinada. She has 9 years of teaching experience. Her area of Interest is Networking.