A REVIEW ON VARIOUS SECURITY FLAWS AND THEIR POSSIBLE COUNTER MEASURES OVER WIRELESS SENSOR NETWORK

Ankita Rana[1],Er. Ankita Mittal[2]

[1] *Student,CSE,Galaxy Global group of Institutions, Sahabad Markanda, Haryana, India*
[2] *Assistant Professor, CSE,Galaxy Global group of Institutions, Sahabad Markanda, Haryana, India*

ABSTRACT

In the near future, sensor networks are going to be a part of everyday life. Traffic monitoring, military tracking, building safety, pollution monitoring, wildlife monitoring, patient security are some of the applications in sensor networks. Sensor networks vary in size and can consist of 10 to 1,000,000 sensor nodes. They can be deployed in a wide variety of areas, including hostile environments, demanding secure measures for data transfer. Sensor nodes used to form these networks are resource-constrained, which makes these types of security applications a challenging problem. A basic technique to protect data is encryption; but, due to resource constraints, achieving necessary key agreement for encryption is not easy. Cryptographic and authentication protocols have been proposed to protect these networks from outsider intrusions but fail to protect them from the insider ones. most of them focus on the anomaly detection in general assuming that the intrusion is kind of anomalies.

Keyword: - *WSN, AODV, MAC etc….*

1. INTRODUCTION

A. Wireless Sensor Network

Wireless Sensor Networks (WSN) can be defined as self-configured and infrastructure less wireless network made of small devices equipped with specialized sensors and wireless transceivers. Sensor networks represent a new frontier in technology that holds the promise of unprecedented levels of autonomy in the execution of complex dynamic missions by harnessing the power of many inexpensive electromechanical microdevices. A sink or base station acts like an interface between users and the network. One can retrieve required information from the network by injecting queries and gathering results from the sink. Typically a wireless sensor network contains hundreds of thousands of sensor nodes. The sensor nodes can communicate among themselves using radio signals [7].

A wireless sensor node is equipped with sensing and computing devices, radio transceivers and power components. The individual nodes in a wireless sensor network are inherently resource constrained: they have limited processing speed, storage capacity, an communication bandwidth. After the sensor nodes are deployed, they are responsible for self-organizing an appropriate network infrastructure often with multi-hop communication with them. Then the on board sensors start collecting information of interest. Wireless sensor devices also respond to queries sent from a control site to perform specific instructions or provide sensing samples. The working mode of the sensor nodes may be either continuous or event driven.

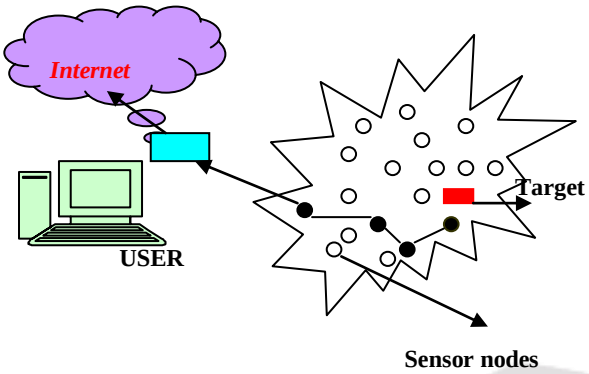

Figure 1.1: General Architecture of a Wireless Sensor Network.

B. Wireless sensor Node Architecture

The architecture of a wireless sensor device is very simple. A WSN is composed of three main functional units: a sensing unit, a communication unit and a computing unit. General architecture of a wireless sensor node is, as shown in figure 1.2. These different elements of wireless sensor nodes are as follows [6, 8]:

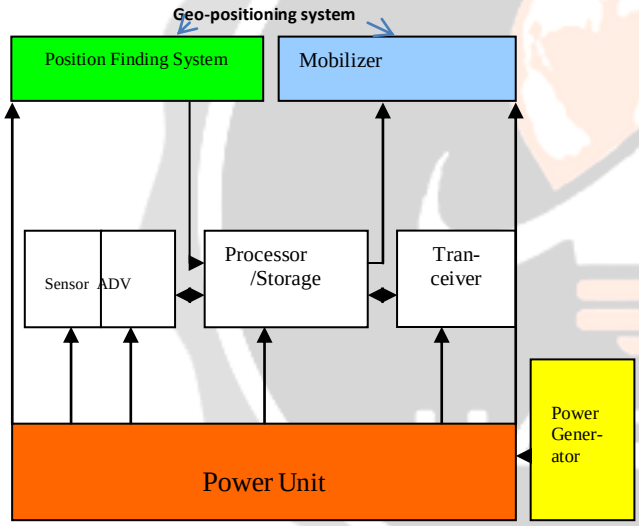

Figure 1.2: General Architecture of a Wireless Sensor Node

- *Processor:*
  The computational tasks on a WSN device include the processing of both locally sensed in-formation as well as information communicated by other sensors. Processor may also incorporate advanced low power design techniques, such as efficient sleep modes and dynamic voltage scaling to provide significant energy savings.
- *Memory/storage:*
  Storage in the form of random access and read-only memory includes both program memory and data memory. The quantities of memory and storage on board a WSN device are often limited primarily by economic considerations, and are also likely to improve over time.
- Transceiver:

WSN devices include a low-rate, short-range wireless radio (10–100 kbps, <100 m). Radio communication is often the most power intensive operation in a WSN device, and hence the radio must incorporate energy-efficient sleep and wake-up modes.

- *Sensors:*

  Due to bandwidth and power constraints, WSN devices primarily support only low-data-rate sensing. The specific sensors used are highly dependent on the application; for example, they may include temperature sensors, light sensors, humidity sensors, pressure sensors, accelerometers, magnetometers, chemical sensors, acoustic sensors, or even low-resolution imagers.

- *Geo-positioning system :*

  In many WSN applications, it is important for all sensor measurements to be location stamped. The simplest way to obtain positioning is to pre-configure sensor locations at deployment, but this may only be feasible in limited deployments. Particularly for outdoor operations, when the network is deployed in an *ad hoc* manner, such information is most easily obtained via satellite-based GPS. However, even in such applications, only a fraction of the nodes may be equipped with GPS capability, due to environmental and economic constraints. In this case, other nodes must obtain their locations indirectly through network localization algorithms.

- *Power Generator:*

  For flexible deployment the WSN device is likely to be battery powered. While some of the nodes may be wired to a continuous power source in some applications, and energy harvesting techniques may provide a degree of energy renewal in some cases, the finite battery energy is likely to be the most critical resource bottleneck in most WSN applications.

B. Classification af Attacks

The special properties of ad hoc networks enable all the neat features such networks have to offer, but at the same time, those properties make implementing security protocols a very challenging task. One of the fundamental vulnerabilities of WSNs comes from their open peer-to-peer architecture. Unlike wired networks that have dedicated routers, each mobile node in an ad hoc network may function as a router and forward packets for other nodes. The wireless channel is accessible to both legitimate network users and malicious attackers. As a result, there is no clear line of defense in WSNs from the security design perspective. The boundary that separates the inside network from the outside world becomes blurred. There is no well-defined place or infrastructure where we may deploy a single security solution. There are four main security problems that need to be dealt with in ad hoc networks:

(1) the *authentication* of devices that wish to talk to each other;
(2) the *secure key establishment* of a session key among authenticated devices;
(3) the *secure routing* in multi-hop networks; and
(4) the *secure storage of (key)data* in the devices.

B. Security Attacks

Security attacks can be classified in different ways. One way is to divide attacks into four categories according to where the attacker deploys the attack in the flow of information from a source to a destination.

- **Interruption:** An asset of the network is destroyed or becomes unavailable or unusable. This is an attack on availability. Examples include silently discarding control or data packets.
- **Interception:** An unauthorized node gains access to an asset of the network. This is an attack on confidentiality. Examples include eavesdropping control or data packets in the networks.
- **Modification:** An unauthorized node not only gains access to but tampers with an asset. This is an attack on integrity. Examples include modifying control or data packets.
- **Fabrication:** An unauthorized node inserts counterfeit objects into the system. This is an attack on authenticity. Examples include inserting false routing messages into the network or impersonating other node.

A more useful categorization of these attacks is in terms of passive attacks and active attacks :

- **Passive attacks:** A passive attack does not disrupt the operations of a routing protocol, but only attempts to discover valuable information by eavesdropping, or silently discard messages received. Three types of passive attacks are release of message contents, traffic analysis, and message dropping.

- **Active attacks:** An active attack involves modification of the contents of messages or creation of false messages. It can be subdivided into four categories masquerade, replay, modification of messages, and denial of service.

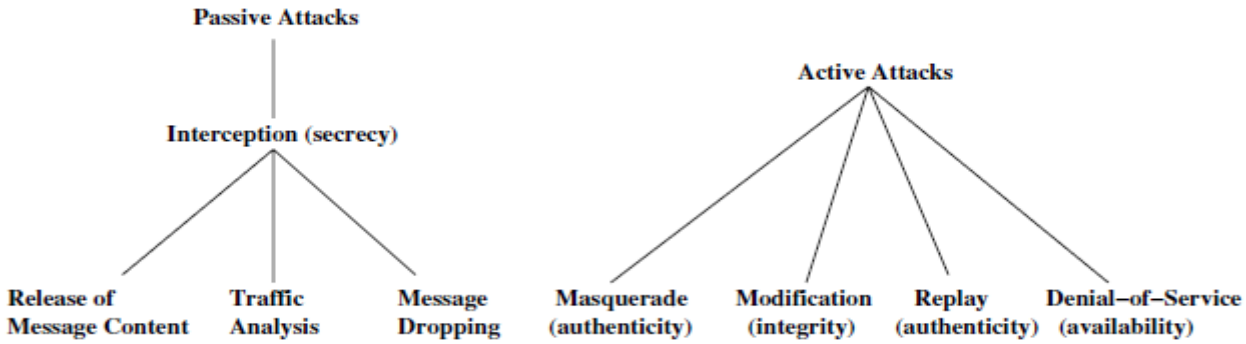

Figure 1.3: Categorization of Attacks.

C. Security mechanisms

A variety of security mechanisms have been invented to counter malicious attacks. The conventional approaches such as authentication, access control, encryption, and digital signature provide a first line of defense. As a second line of defense, intrusion detection systems and cooperation enforcement mechanisms implemented in MANET can also help to defend against attacks or enforce cooperation, reducing selfish node behavior.

- **Preventive mechanism:** The conventional authentication and encryption schemes are based on cryptography, which includes asymmetric and symmetric cryptography. Cryptographic primitives such as hash functions (message digests) can be used to enhance data integrity in transmission as well. Threshold cryptography can be used to hide data by dividing it into a number of shares. Digital signatures can be used to achieve data integrity and authentication services as well. It is also necessary to consider the physical safety of mobile devices, since the hosts are normally small devices, which are physically vulnerable. For example, a device could easily be stolen, lost, or damaged. In the battlefield they are at risk of being hijacked. The protection of the sensitive data on a physical device can be enforced by some security modules, such as tokens or a smart card that is accessible through PIN, passphrases, or biometrics. Although all of these cryptographic primitives combined can prevent most attacks in theory, in reality, due to the design, implementation, or selection of protocols and physical device restrictions, there are still a number of malicious attacks bypassing prevention mechanisms.
- **Reactive mechanism:** An intrusion detection system is a second line of defense. There are widely used to detect misuse and anomalies. A misuse detection system attempts to define improper behavior based on the patterns of well-known attacks, but it lacks the ability to detect any attacks that were not considered during the creation of the patterns; Anomaly detection attempts to define normal or expected behavior statistically. It collects data from legitimate user behavior over a period of time, and then statistical tests are applied to determine anomalous behavior with a high level of confidence. In practice, both approaches can be combined to be more effective against attacks. Some intrusion detection systems for MANET have been proposed in recent research papers.

2. RELATED WORK

I Karkazis et al. [1], proposed formulas for quantifying primary routing metrics which capture effects relevant to the considered network type and of interest to the applications they serve and we investigated their combinations in additive or lexicographic composite routing metric lead to loop-free routing protocols which converge to optimal paths. The authors design primary routing metrics which (a) capture WSN relevant node and network characteristics (b) are proved to be monotonic and strictly isotonic and (c) are suitable for building composite metrics to meet diverse application requirements still satisfying the monotonicity and strict is tonicity requirements so that the routing protocol converges to optimal paths in a loop-free manner To evaluate the performance benefits brought by the combination, the authors have run scenarios for different composite routing metrics combining HC and PFI for different penetrations of misbehaving nodes randomly distributed in the grid. The misbehaving nodes perform ‘‘*grey hole attacks*”, i.e. drop randomly half of the received traffic and are randomly distributed in the network in the 50 different repetitions of each scenario. From extensive simulation results, the authors analysed the performance

difference between different composite routing and primary metrics. Based on these results, the authors also provides guidelines and examples of routing metrics that seem to better suit specific applications.

Haifeng Yu [2], proposed a novel *tree sampling* algorithm that directly uses sampling to answer aggregation queries that enables it to tolerate instead of just detecting the adversary. Sampling of individual sensors is used in for detecting corrupted aggregation results, instead of computing the result. Sampling of individual sensors is also used in trusted environments to catch big events .Tolerating the adversary is typically much harder than simply detecting it. Most of the protocol can only *detect* but not *tolerate* malicious sensors. Typical security Techniques enable the user to verify whether the result is corrupted. But even a *single* malicious sensor can keep preventing the verification from succeeding, in which case the user can never get a correct result. The author designed a protocol with provable guarantees that can always correctly answer aggregation queries despite adversarial interference. This algorithm leverages a set sampling protocol which can efficiently sample a set of sensors together and determine whether any sensor in the set satisfies the predicate With set sampling, each node on the decision tree corresponds to a query specifying some subset of the bits, and invoking the query will determine whether any bits in the subset. Here author consider n = 10,000 sensors. The adversary compromises g = 0 to 5,000 sensors out of them. Among the n−g honest sensors, author supposed to set the number of black sensors b = 5,000, while the remaining n−g−b sensors are white. Because some sensors are now compromised, some of the keys on the sampling tree are grey. The author have also experimented with the alternative strategy where all grey keys at odd levels test white and all grey keys at even levels test black.

Jaydip Sen [3], presented a brief outline on the constraints of WSNs, security requirements in these networks, and various possible attacks and the corresponding countermeasures. These issues are classified into six categories: cryptography, key management, secure routing, secure data aggregation, intrusion detection and trust management. The advantages and disadvantages of various security protocols are discussed, compared and evaluated. Since WSNs are capable of automatic data collection through efficient and strategic deployment of sensors, these networks are also vulnerable to potential abuse of these vast data sources. Privacy preservation of sensitive data in a WSN is particularly difficult challenge. The privacy preservation in WSNs is even more challenging since these networks make large volumes of information easily available through remote access mechanisms. A number of key management protocols for WSNs are discussed next. The author discussion various methods of defending against DoS attacks, secure broadcasting mechanisms and various secure routing mechanisms.

Ana Maria Popescua et al. [4], presented a brief comparsion of almost 50 position-based routing protocols for both ad-hoc and wireless sensor networks, in both static and mobile scenarios and also proposes a number of protocols for use in particular application areas. Geographic routing is an elegant way to forwardpackets from source to destination in very demanding environments without wasting network resources or creating any impediment in the network design. Position-based routing altogether can be used for a very high number of applications in a number of areas such as industry, home, health, environmental, military, automotive and commerce. From monitoring and control of industrial equipment, to emergency situation surveillance and physical world surveillance, any application needs a network design with robust routing, with a high expectation of packet delivery, successful route discovery even in mobile scenarios and capability to maintain connectivity for as long as possible without manual intervention. Problems may appear during routing such as packet cycling around the network without reaching their destination, packets being dropped and

never being retransmitted due to node failure, package copies being transmitted in the network redundantly, consuming energy unnecessarily. Geographic routing represents the algorithmic process of determining the paths on which to send traffic in a network, using position information/geographic location only about source, neighbours and destination. This survey paper suggests which protocols are most suitable for certain applications. It also helps in understanding the steps made in the design of position-based routing protocols for highly demanding network applications and which aspects still require a lot of attention. While some protocols guarantee delivery, have

excellent delivery ratio, look promising from the mobility point of view or seem satisfactory regarding memory availability, they still need a lot of improvement in other areas.

V. Geetha et al. [5], propose a parameter and trust factor based secure communication framework and design a trust management system for wireless sensor networks. The trust of a neighbour node is calculated based on evaluation of trust factors. Each trust factor is evaluated based on observed parameters. To calculate trust between two nodes, a node has to observe its neighbour for its interactions with node . The authors have identified total six groups of data to be observed on the network. The results are analyzed for 10%, 20% and 30% attacker nodes. The metrics used for comparison of results is based on True Positive (TP), True Negative (TN), False Positive (FP) and False Negative (FN). The results are compared to standard Bayesian trust model (STM) with exponential decrease Bayesian trust model (ETM). The simulation results show that the proposed model works for secure communication, data aggregation and intrusion conducted in MATLAB for the application of secure communication, data aggregation and intrusion detection in wireless sensor networks.

Adnan Ahmed et al. [6], comprehensively investigates the performance of AODV protocol by simulating it on the various network parameters with various number of blackhole nodes. AODV is source initiated, reactive and loop free routing protocol which creates route between source and destination when needed. AODV differs from its counterpart proactive routing protocols since in proactive routing updates are send periodically that leads to high overhead. The authors evaluates the performance of AODV routing protocol in presence of various number of blackhole nodes using Network Simulator 2 (NS2). The performance analysis is performed with the four conditions. First, there is no blackhole node in the network. Second, 1 node is compromised.· Third, there are two nodes thatbehave as blackhole nodes· Fourth, there are three nodes behave as blackhole nodes. The authors have compared AODV with compromised AODV in terms of normalized routing load, packet delivery ratio, end to end delay and packet drop ratio.

Smita Karmakar et al.[7], present a brief comparative study of various types of holes and various types of coverage holes. Holes are one of the challenges in deployment of WSNs in a large area. Holes generally considered as a communication gap among sensor nodes. The authors also provides a brief overview two different solutions for hole detection that are proposed by researchers. They are vornoi diagram and triangular oriented diagram. Voronoi diagram approach is used to detect a coverage hole and calculate the size of a coverage hole. A plane area is divided into N cells. Each cell contains one sensor. Two Voronoi cells meet along a voronoi edge. A sensor node is a voronoi neighbour of other sensor node, if they both share a voronoi edge. Voronoi diagram approach has few limitations like shape of each cell is different. So, it is very tough to calculate the exact size of the hole. The limitation of other solution namely triangular oriented structure is that, it is not a proper hole detection solution because, in a large WSNs, it is complex to connect the centre of three adjacent sensors. Here authors also proposed simple and straight-forward algorithm initially find out whether a sensor node is alive or dead. According to this algorithm, when the sensor node is dead, then the geographical area is not covered by that sensor node, so this area will be treated as hole.

Benamar Kadri et al. [8], propose a lightweight implementation of public key infrastructure called cluster based public infrastructure (CBPKI). CBPKI is based on the security and the authenticity of the base station for executing a set of handshakes intended to establish session keys between the base station and sensors over the network used for ensuring data confidentiality and integrity. CBPKI is intended to establish security over the network using three cryptographic methods destined to establish all the security services. CBPKI is based on two handshakes namely Cluster-head to base station handshake and Cluster members handshake. The handshake is executed by each cluster head and the base station is intended to establish a symmetric key be-tween sensors and the base station. propose to launch periodically a proactive key update of the session key; the period of the key update is defined by the administrator according to the length of the used keys as well as the robustness of the encrypting algorithms. The key update is launched by the cluster head using the same hand shake defined above in order to establish a new session key between the base station and the cluster head. After updating the session key of the cluster head, each cluster head encrypts a copy with the old session key for each member of its cluster. The authors also ensures the

CBPKI for all security services and checks its robustness against several attacks with low power consumption and network overhead.

3. CONCLUSIONS

In this paper, We covered general denial of service Various possible threats and attacks on sensor networks and their possible prevention. The security schemes that govern trust among communicating entities are collectively known as trust management. Here trust means the confidence of an entity on another entity based on the expectation that the other entity will perform a particular action important to the one who trusts, irrespective of the ability to monitor or control that other entity. In the trust management system, reputation system and other trust-based systems, route selection is based on the sending node's prior experience with other nodes in the network. By incorporating the dynamic feedback mechanism in the routing protocol, misbehaved nodes are identified and avoided to forward packets. In this way, misbehavior can be mitigated

REFERENCES

[1]. Panagiotis Karkazis, Panagiotis Trakadas, Helen C. Leligou, "Evaluating routing metric composition approaches for QoS differentiation in low power and lossy networks" Wireless Network, Springer, December 2012.

[2] Haifeng Yu, "Secure and highly-available aggregation queries in large-scale sensor networks via set sampling" Distributed Computing, Springer , February 2011.

[3] Jaydip Sen, "A Survey on Wireless Sensor Network Security" International Journal of Communication Networks and Information Security, August 2009, pp. 59-82.

[4] Ana Maria Popescua, Ion Gabriel Tudorachea, Bo Pengb and A.H. Kempa, "Surveying Position Based Routing Protocols for Wireless Sensor and Ad-hoc Networks" International Journal of Communication Networks and Information Security, Vol. 4, No. 1, April 2012, pp. 41-67.

.[5] V. Geetha and K. Chandrasekaran, "A Distributed Trust Based Secure Communication Framework for Wireless Sensor Network "Wireless Sensor Network, scientific research, 2014, pp. 183-183.

[6] Adnan Ahmed, Kamalrulnizam Abu Bakar and Muhammad Ibrahim Channa, "PERFORMANCE ANALYSIS OF ADHOC ON DEMAND DISTANCE VECTOR PROTOCOL WITH BLACKHOLE ATTACK IN WSN" Journal of Computer Science, Science Publications, ISSN: 1549-3636, 2014, pp. 1466-1472.

[7] Smita Karmakar and Alak Roy, "Holes Detection in Wireless Sensor Networks: A Survey" Modern Education and Computer Science, MECS, 2014, pp. 24-30.

[8] Benamar Kadri, Djilalli Moussaoui, Mohammed Feham and Abdellah Mhammed, "An Efficient Key Management Scheme for Hierarchical Wireless Sensor Networks" Wireless Sensor Network,Scientifi research, June 2012, pp. 155-161.