International Journal of Engineering and Advanced Technology (IJEAT)
ISSN: 2249-8958 (Online), Volume-4 Issue-5, June 2015

Security Breaches and their Solutions in WSN

Md. Aleemuddin Ghori, Syed Abdul Sattar

Abstract: - Wireless sensor network is an upcoming technology and are getting Popularity quickly and a lot of attention because of their low cost solutions to a number of large sensor arrays, and capable to implement in military as well as for civilians. This technology has many applications including various environmental monitoring; target tracking, scientific exploration, patient monitoring and tracking, and data acquisition in hazardous environments. Sensor nodes are deployed in a hostile locations security becomes extremely important. They have limited data storage and power capacity because of their small size and this is the major limitation to implement the traditional computer security methods. The unpredictable communication channel and unattended operation make the security defenses harder. In this paper we have discussed the importance of security breaches and their solutions.

Keywords: Popularity quickly, large sensor arrays, various environmental monitoring; target tracking, scientific exploration, patient monitoring.

I. INTRODUCTION

Risk Analysis:-- WSN are inherently resource constrained as they have limited processing power and limited storage capacity and a short-range communication bandwidth. Each of these limitations is due to limited energy and small size. On the other hand the monitoring locations where the sensor network technology is being employed are usually hostile in nature and are prone to different types of malicious attacks where an enemy can compromise the sensor node and launch hazardous attacks from there [1]. This security vulnerability adds a new challenge to the design of secure mechanisms for sensor networks. Detecting such vulnerabilities is considered a crucial task. In our work we outline major security attacks and their counter measures.

II. COMMON SECURITY ATTACK ON WIRELESS SENSOR NETWORKS

1.1 Physical attacks:

Sensor networks usually operate in hostile sensitive locations in such surroundings the minimality of the sensors coupled with the unattended and distributed nature of their placement make them highly susceptible to physical attacks [2].Physical attacks may destroy sensors permanently and the losses can be irreversible for example attackers can extract cryptographic secrets and tamper with the associated circuitry further can modify programming in the sensors or replace them with malicious sensors under the control of the attacker. Therefore the security schemes for sensor networks should be resistant to node capture.

Manuscript published on 30 June 2015.
***** Correspondence Author (s)
Dr. Md Aleemuddin Ghori, Professor in Department of CSE, Royal Institute of Technology & Science, Chevella RR Dist., TS. India.
Dr. Syed Abdul Sattar, Professor & Dean of Academics, Royal Institute of Technology & Science, Chevella RR Dist., TS. India.

1.2 Attacks on authenticity and integrity:

Without proper authentication mechanisms, unauthorized people or malicious users could also try to join the network undetected by imitating as a trusted node[3] and this will now have access to private data or it can interrupt the normal network operations. Therefore the security schemes employed should be assured that sensor readings are transferred from sensor nodes to the base station without any modification by the intruders Otherwise wrong data will be processed resulting in improper decisions taken in operation centers and this might have disastrous effects such as guiding military troops to the wrong side of the battlefield.

1.3 Attacks on privacy:

One of the most common attacks on privacy is monitoring and eavesdropping through listening to the data and the opponent could easily determine the message contents. When the traffic carries the control information about the sensor network configuration which contains potentially more detailed information available in the server the eavesdropping can act efficiently against the privacy in wireless sensor networks [4]. Enemies could use even apparently insensitive data to derive sensitive Information easily through remote access without actually present to maintain surveillance and can gather information in a safely and in a mysterious manner and could Supply the misleading information to the victim.

1.4 DoS Attacks:

A DoS attack reduces a network's capacity to perform its normal task. DoS attack tries to exhaust the resources available to the victim node by sending extra unnecessary packets and hence stops legitimate network users from accessing the services or resources to which they are permitted [5]. DoS attacks on sensor networks range from simple jamming of sensor's communication channel to more sophisticated attacks. DoS attacks can be very dangerous when sensor networks are used in highly critical and sensitive applications. A very common denial-of-service attack specific to sensor networks is battery power exhaustion. Limited battery life is the acute constraint for the nodes in a sensor network to be considered and many methods are used to maximize it. For example, nodes try to spend most of the time in a sleep mode in which they only turn on the radio receiver or even the processor once in a while. In this situation, energy exhaustion attacks are a real threat and hence lacking adequate security a malicious node could disallow another node to go back to sleep producing the battery to be shattered. Even though there are numerous solutions to lessen DoS for traditional networks but sensor networks cannot afford the computation overhead desired in applying those methods.

Published By:
Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP)

1.5 Wormhole attack:

In the wormhole attack a malicious node tunnels packets received from one part of the network in a low latency link and replays them in a different portion [6]. Wormhole attack usually involves two distant malicious nodes uniting to minimize distance between them by transmitting the packets along an out-of-band channel. A rival situated close to a base station can totally interrupt routing by creating a well-placed wormhole. The opponent can fool nodes who are mostly multiple hops from a base station that they are only one or two hops away via the wormhole. Meanwhile the malicious node on the other side of the wormhole can falsely provide a high class route to the base station all traffic in the neighboring area will be drained through it if the substitute routes are less attractive then this will be most likely be the case when the endpoint of the wormhole is comparatively distant from a base station.

1.6 Sinkhole attack:

In a sinkhole attack [7] the enemy's goal is to trap nearly all the traffic from a specific area through a compromised node creating a Figurative sinkhole with the adversary at the center. Because nodes on, the path that packets follow have many chances to tamper with application data, sinkhole attacks can permit many other attacks like selective forwarding. Sinkhole attacks typically work by making a compromised node look especially striking to surrounding nodes with respect to the routing algorithm. For instance, an opponent could spoof or replay an advertisement for an extremely high quality route to a base station.

1.7 Sybil attack:

In case of a Sybil attack [8] a single node presents several identities to other nodes in the network and Sybil attacks also pose a threat to geographic routing protocols which involve nodes to exchange location information with their neighbors. It is sensible for a node to accept only a single set of coordinates from each of its neighbors but by using the Sybil attack a malicious node can pretend to be in more than one place simultaneously. Sybil attack attempts to degrade the integrity of data degrade security and resource utilization that the distributed algorithm tries to achieve. Sybil attacks are used as a weapon for attacking the distributed storage, routing mechanism, data aggregation and fair resource allocation.

1.8 HELLO flood attack:

In a HELLO flood attack an attacker broadcasting HELLO packets to announce itself with bulky adequate transmission power could influence every node in the network that the adversary is its neighbor. For instance a malicious node advertising a very high-quality route to the base station might cause a large number of nodes to attempt to use this route but those nodes sufficiently far away from the opponent would be sending packets into a nullity. The network can enter into a state of confusion [9]. Even if a node understands the link to the enemy is false it does not have several options because all its neighbors might be attempting to forward packets to the adversary as well. Protocols which depend on localized information exchange between neighbor nodes for topology maintenance or flow control are also subject to this attack.

1.9 Selective forwarding:

In a selective forwarding attack the nasty nodes might decline to forward certain messages and just drop them with the aim that they are not propagated any further. The simplest form of this attack is when a malicious node acts like a black hole and refuses to forward any packet. But in that case neighboring nodes may conclude that malicious node has failed and decide to seek another route [10]. A more subtle form of this attack is once an opponent selectively forwards packets a malicious node involved in destroying or altering packets initiating from a particular node can consistently forward the remaining traffic and hide suspicion of its wrongdoing.

1.10 Acknowledgement spoofing:

Most of the WSN routing algorithms depend on implicit or explicit link layer acknowledgements a routing protocol may select the next hop in a path based on link reliability [11]. with this an adversary try to convince the sender that a fragile link is robust or a dead or disabled node is alive and the packets sent along the weak or dead links are lost and the challenger can launch a selective forwarding attack using acknowledgement spoofing by reinforcing the target node to transmit packets on those links and in this way an enemy can spoofed link layer acknowledgments for overheard packets addressed to neighbor nodes thereby enforcing an attack.

III. PROPOSED SOLUTIONS

When targeting at security for Wireless Sensor Networks one has to focus primarily on protecting the traffic. Some recent proposals support the encryption of converge-cast traffic with in the network processing. But they either require the transmission of the sensors' IDs, creating additional data overhead or require an elaborate key pre-distribution mechanism. In our proposed solution we have defined security and consistency trials for WSNs. Link layer encryption and authentication mechanisms may be considerably the better defense against mote-class outsiders but cryptography alone is not adequate and the existence of laptop-class adversaries and the limited applicability of end-to-end security mechanisms demands vigilant design of the protocol. Providing the identity verification bidirectional link verification and authenticated broadcast can protect sensor network routing protocols against outsiders. Effective methods are essential to counter the Sinkhole and wormholes attacks as they possess the extensive encounter. In a multihop routing topology around a fixed set of base stations nodes within one or two hops of the base stations are particularly attractive for compromise and after a significant number of these nodes have been compromised then the enemy could get enough knowledge to harm the entire network. The clustering protocols like LEACH where cluster-heads communicate directly with a base station may most desired secure solutions against compromising the node and insider attacks. Another option may be to have a randomly rotating set of virtual base stations to create an overlay network and the virtual base stations could directly communicate with the real base stations and these set of virtual base stations should be changed frequently making it hard for adversaries to choose the required nodes for attacks.

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

To provide better Security and have the less damage each sensor node should be equipped with a tamper-resistant component to store the sensitive data but this is not possible because of the high cost so we can think of probabilistic security approach where the attacker gains limited knowledge which is unsueful to launch severe attacks.

IV. CONCLUSION

Due to the unique challenges pretended by sensor networks, traditional security techniques cannot be directly applied. It is very important to build a secure channel in wireless sensor network public sensor information such as sensor identities and public keys should also be encrypted to some level to safeguard against traffic analysis attacks. Shared keys need to be changed over time and asymmetric mechanisms are required to achieve authenticated broadcast.

REFERENCES

[1] E. Mykletun, J. Girao, D. Westhoff "Re-visited Public key based crypto schemes for data concealment in Wireless Sensor networks " IEEE ICC, Turkey May 2006
[2] D. Westhoff J. Girao M. Acharya "concealed data aggregation for Reverse multicast Traffic in Sensor Networks Encryption "Key Distribution and Routing Adaptation IEEE Transactions on Mobile Computing in 2006
[3] A. Becher. Benenson and Dornseif Tampering with motes real-world physical attacks on wireless sensor networks 2006.
[4] M. Acharya, J. Girao, D. Westhoff "Secure Comparison of Encrypted Data in Wireless Sensor Networks " 3rd WiOpt, April 2005
[5] Chris karlof and David Wagner. Secure routing in wireless sensor networks Attacks and countermeasures. Elsevier's Adhoc Networks Journal, Special Issue on Sensor network applications and Protocols 293_315, Sept 2003.
[6] A. Weimerskirch D. Westhoff "Zero-Common Knowledge Authentication for Pervasive Networks 10th Selected areas in Cryptography SAC ' 03 Springer-Verlag LNCS 3006, pp.73-87, Ottawa, Ontario, CA August 2003
[7] Y.-C. Hu A. Perrig D.B. Johnson Packet leashes a defense against wormhole Attacks in wireless networks in IEEE Info com, 2003.
[8] J. R Douceur. The Sybil attack in 1st International Workshop on Peer-to-peer Systems (IPTPS _02), 2002.
[9] Y.C. Hu, A. Perrig, D.B. Johnson Ariadne a secure on demand routing Protocol for adhoc networks in MOBICOM, 2002.
[10] D. Dolev A.C. Yao "On the security of Public-Key Protocols " IEEE Transactions on Information Theory 29(2):198-208, 1983
[11] S. Rajasegarar, C. Leckie, and M. Palansiwami, "Anomaly detection in wireless sensor networks", IEEE Wireless Communications, vol. 15, no. 4, Aug. 2008, pp. 34-40

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)