International Journal of Innovative Research in Science and Engineering
Vol. No.3, Issue 01, January 2017
www.ijirse.com
ISSN (O) 2454-9665
ISSN (P) 2454-0663

SECURE ROUTING IN WIRELESS SENSOR NETWORKS: ATTACKS AND COUNTMEASURES

S Jagadeesan, Dept. of CSE, SRM University (India)

ABSTRACT

Wireless detector Networks (WSN) unit rising technology now-a-days and includes a big selection of applications like traffic police investigation fire detection flood detection. Wireless detector networks unit vulnerable to a range of potential attacks that obstructs the conventional operation of the network. This paper focuses on varied attacks that manifest within the network and provides a tabular illustration of the attacks, their effects and severity. Thanks to restricted resources of battery, computation power, communication vary, etc., WSN is susceptible to differing types of attacks. A comparison of attacks basis packet loss and packet corruption. The paper discusses the best-known defense mechanisms and countermeasures against the attacks. This paper discusses best-known approaches of detection and defensive mechanisms against the routing attacks; this might alter it security managers to manage the routing attacks of WSNs additional effectively.

Keywords: WSN, Varieties of Attacks, Security Countermeasures, Routing Protocol.

I INTRODUCTION

A device network contains a gaggle of small, usually powered devices and wireless infrastructure that monitor and record conditions in a range of environments from the plant floor to the info center in a hospital laboratory and even get in the wild. The device network connects to the net, AN enterprise WAN or computer network, or a specialized industrial network in order that collected knowledge may be transmitted to back-end systems for analysis and employed in applications. A network device consists of multiple detection stations known as device nodes, every of that is tiny, lightweight and transportable. Each device node is provided with an electrical device, personal computer, transceiver and an influence supply. The electrical device generates electrical signals supported perceived physical effects and phenomena. The personal computer processes and stores the device output. The transceiver receives commands from a central PC and transmits knowledge thereto PC. The facility of every device node springs from electric battery.

The technological advancements in wireless communication and electronics have resulted in a very growing interest within the field of wireless device networks. A device network involves deploying AN array of sensors for the distributed watching of real time events. The device networks have restricted energy, because the device nodes area unit battery steam-powered. The device nodes even have restricted memory and procedure capability and may be deployed in remote areas or inhospitable piece of land. There has been AN increasing use of device networks for all times crucial applications like watching patients in hospitals and military applications. These applications are build

ISSN (O) 2454-9665
ISSN (P) 2454-0663

it necessary to own a decent security infrastructure for device networks. The readying of those networks in military applications and also the restricted power and memory, build the look of a security protocol terribly difficult. During this paper security issue in Directed diffusion area unit self-addressed. Directed Diffusion may be a novel routing protocol for device networks. A log-in to potential attacks and countermeasures is provided. The directed diffusion protocol followed by a discussion of the potential attacks on this routing protocol. The paper concludes with a quick analysis on the potential countermeasures to stop such attacks.

WSNs were at the start designed to facilitate military operations, however, its application has since been extended to health, traffic, and plenty of alternative shopper and industrial areas. A WSN consists of anyplace from some lots of to thousands of device nodes. The device node instrumentation includes a radio transceiver in conjunction with AN antenna, a macrocontroller interfacing electronic circuit, ANd an energy supply, sometimes electric battery. The dimensions of the device nodes may also vary from the dimensions of a shoe box to as tiny because the size of a grain of dirt. As such, their costs additionally vary from some pennies to many greenbacks counting on the practical parameters of a device like energy consumption, procedure speed rate, bandwidth, and memory. Potential applications of device networks include: Industrial automation, machine-driven and sensible homes, Video police work, Traffic watching, Medical device watching, watching of weather, traffic management and management mechanism.

Why security required in wireless device networks WSNs are getting a value effective, sensible thanks move deploying device networks. Massive variety of applications from civilian to military functions. Create completely different challenges as compared to ancient networks. Security threats area unit impending thanks to the open nature of communication. 2 main issues: authentication and privacy. Alternative serious issues: denial-of-service. The most aspects area units.

II WSN SECURITY GOALS

Shares some common points with traditional networks, but also presents unique problems of its own.

Data confidentiality: A set of rules that limits access to information. A very key component of protecting information confidentiality would be encrypted. Encryption ensures that only the right people can read the information. A security protocol for communications over the internet that has been used in conjunction with a large number of internet protocols to ensure security.

Data integrity: Integrity of information refers to protecting information from being modified by unauthorized parties. To protect data integrity includes hashing the data you receive and comparing it with the hash of the original message. The hash of the original data must be provided to you in a secure fashion.

Data freshness: Ensures that no old messages have been replayed.

Availability: To ensuring that authorized parties are able to access the information when needed. a term used by computer storage manufacturers and storage service providers (SSPs) to describe products and services that ensure that data continues to be available at a required level of performance in situations ranging from normal.

ISSN (O) 2454-9665
ISSN (P) 2454-0663

Authentication: The process of identifying an individual usually based on a username and password. Authentication is any process by which a system verifies the identity of a User who wishes to access it. Authentication may be implemented with Smart Cards, an Authentication Server or even a Public Key Infrastructure.

Access control: Access control is a security technique that can be used to regulate who or what can view or use resources in a computing environment. There are two main types of access control: physical and logical. Physical access control limits access to campuses, buildings, rooms and physical IT assets. Logical access limits connections to computer networks, system files and data.

III SECURITY CHALLENGES IN WSN

Eavesdropping caused by abuse of routing protocol is that the responsibility of protocols. The challenges of coming up with and implementing of a secure routing in WSN area unit the vulnerability of the network to eavesdropping, spoofing, unauthorized access, and DOS attacks will increase attributable to the wireless communication among the detector nodes. The restricted resource constraint of the detector nodes, like memory, CPU, bandwidth, and battery life, hinders the degree of implementation of coding, coding and authentication mechanisms in individual detector nodes. The physical security risk of being deployed within the field individual detector nodes will be obtained associate degrees face attacks from an unauthorized user so as to compromise one detector node. This completely different mechanism should be chased and massive analysis potential.

3.1 Attacks on Wireless Sensor Network Routing

Spoofed, altered, or replayed routing information

This is the most direct attack against a routing protocol. Adversaries may be able to create routing loops, attract or repel network traffic, extend or shorten source routes, generate false error messages, partition the network, increase end-to-end delay latency.

Selective Forwarding

Malicious nodes may refuse to forward certain messages, drop them, ensuring that they are not propagated any further. In order not to get noticed by the neighboring nodes by not forwarding the packets, the adversary may selectively forward the packets. It is most effective when the attacker is openly included in the path of a data flow. A challenger overhearing a flow passing through neighboring nodes might be able to emulate selective forwarding by jamming or causing a collision on each forwarded packet of interest.

Sinkhole Attacks

Adversary tries to lure all the traffic from a particular area through a compromised node, creating a metaphorical sinkhole with the adversary at the center. Typically works by making a compromised node look attractive to surrounding nodes with respect to the routing algorithm. The adversary could spoof or replay an advertisement for a

ISSN (O) 2454-9665
ISSN (P) 2454-0663

high quality route to a base station. Due to either real or imagine high quality route through compromised node, each neighboring node of the adversary will forward packets destined for a base station through the adversary. Since all packets share the same destination node needs only to provide a single high quality route to the base station to influence a large number of nodes.

The Sybil Attack

A single node presents multiple identities to other nodes in the network. This type of attack can reduce the effectiveness of fault-tolerant schemes and pose a threat to geographic routing protocols. An adversary can be in more than one place at once by using this attack.

Wormholes

An adversary tunnels messages received one part of the network over a low latency link and replays them in a different part. Wormhole attacks generally involve two distant malicious nodes colluding to understand their distance from each other by relaying packets along an out-of-band channel available only to the attacker. An adversary can convince nodes who are multiple hops away from the base station to believe that they are only one or two hops away via the wormhole creates a sinkhole. Wormholes can be used to convince two distant nodes that they are neighbors by relaying packets between the two of them. This attack can be combined with selective forwarding or eavesdropping.

HELLO Flood Attack

A laptop-class attacker broadcasting routing or other information with large enough transmission power could convince every node in the network that the adversary is its neighbor. An adversary advertising a high quality route to the base station to every node in the network can cause a large number of nodes to use this route, leaving the network in the state of confusion. An adversary can re-broadcast overhead packets with enough power to be received by every node. HELLO floods can be considered as one-way broadcast wormholes and uses a single hop broadcast to transmit a message to a large number of nodes unlike the traditional definition of a flooding denoting epidemic like propagation of a message to every node in the network.

Acknowledgement Spoofing

An adversary can spoof link layer acknowledgements for overhead packets addressed to the neighboring nodes. A sender can be convinced that a weak link is strong or a dead node is alive since packets sent along with weak or dead links are lost. An adversary can mount a selective forwarding attack using acknowledgment spoofing by encouraging the target node to transmit packets on those weak links.

Countermeasures

Link layer encryption and authentication with a symmetric key prevent most outsider attacks. Replay attacks are prohibited by using a rising counter. An attacker can still forward packets without changing. Encryption can create selective forwarding hard, but does nobody to a black hole attack. Insider cannot be prevented to participate in the

ISSN (O) 2454-9665
ISSN (P) 2454-0663

operations of the network and she can masquerade as any node. A solution: nodes share own unique symmetric keys to the base station. Another one presented was limiting the number of neighbors per node attacker cannot form symmetric keys with too many nodes in the network.

Due to the attacks, security must be taken into account in sensor network routing protocols. The most proposed sensor network routing protocols have been designed without security in mind. In the security goals to consider the characteristic of sensor networks, namely resource starved nature very little computational power, such that public key cryptography is expensive to be unusable communication bandwidth is really transmitted and consumes as much power as executing more than 8 million instructions.

Outsider attacks and link layer security

The majority of outsider attacks in Wireless Sensor Network routing protocols can be prevented by simple link layer encryption and authentication using a worldwide public key. The Sybil attack is no longer relevant because nodes are unwilling to admit even a single identity of the adversary. The majority of selective forwarding and sinkhole attacks are not possible because the adversary is prevented from topology. Link layer acknowledgements can now be authenticated. Major classes of attacks not countered by link layer encryption and authentication mechanisms are wormhole attacks and HELLO flood attacks.

The encryption may create some selective forwarding attacks against packets using wormhole. Link layer security mechanisms using a globally shared key are completely ineffective in the presence of insider attacks or compromised nodes.

The Sybil attacks

Using a worldwide shared key allows an insider to masquerade as any node. In the traditional setting might be done using public key cryptography, but generating and verifying digital signatures is beyond the capability of wireless sensor nodes. One of the solutions is every node share a unique symmetric key with a trusted base station. A pair of nearest nodes can use the resultant key to apply an authenticated and encrypted link between them. In order to prevent an around a stationary network and establishing shared keys with every node in the network the base station can reasonably limit the number of neighbors a node is acceptable and send an error message when a node exceed. When a node is compromised, it is restricted to communicating only with verified neighbors. An adversary can still use a wormhole to make a fake connection between two nodes and encourage them, they are neighbors, but the adversary will not be able to eavesdrop on or alter any future connections between them.

HELLO flood attacks

It can be a defense against by verifying the connection before taking a meaningful action based on a message received over that link. The identity authentication protocol is enough to avoid HELLO flood attacks and verify the bi-directionality of the connection between two nodes. For a multiple location in the network a trusted base location

ISSN (O) 2454-9665
ISSN (P) 2454-0663

that limits the number of confirmed neighbors for each node. In this attack on large segments of the network when a small number of nodes have been compromised.

Wormhole and sinkhole attacks

The wormhole and sinkhole attacks are very hard to defend against especially when the two are used in grouping. Wormholes are tough to detect because they use a secret out of band channel unseen of the underlying sensory network. Sinkholes are not easy to secure against in protocols that use advertised information such as an estimate of end-to-end reliability to build a routing topology because this information is unbreakable to validate. Routes that reduce the hop count to a base station are easier to authenticate, but hop count can be completely changed through a wormhole. At what time routes are recognized simply based on the greeting of a packet as in TinyOS beaconing or directed diffusion, sinkholes are simple to make because no information for a protector to prove. Techniques for detecting wormhole attacks are offered, but it requires really fixed time synchronization and infeasible for most wireless sensor networks. Geographic routing protocols construct a topology initiated by a base station are most susceptible to the wormhole and sinkhole attacks. Geographic protocols construct a topology that requires using only local communications and information and with no initiation from the base station. A wormhole is most effective when used to create sinkholes or artificial links that is a magnet for traffic.

Leveraging global knowledge

An important challenge in securing wireless sensor networks inbuilt self organizing and decentralized environment. To understand that no nodes are compromised during operation after first topology is produced and then each node could send information such as an adjacent node and geographic position reverse to a base station. By means of this information the base station can map the topology of the entire network. To account for topology change due to radio interfering or node failure, nodes would periodically update a base station with suitable information. A compromise node advertising its location on a line between the targeted node and a base station will assure the destination for all forwarded packets from that node.

Selective forwarding

A compromised node has an important option of including data flow to launch a selective forwarding attack located near the source or a base station. Multipath routing can be used to counter these types of selective forwarding attacks. Messages routed more paths whose nodes are totally put out of place are completely protected against selective forwarding attacks involving at most n compromised nodes. On the other hand finally disjoint paths may be not easy to generate. The use of many braided paths can grant probabilistic protection against selective forwarding and use only localized information. Allowing nodes to with dynamism decide a packet's after that hop problematically from a set of possible candidates can further diminish the chances of an adversary fast complete control of a data flow.

ISSN (O) 2454-9665
ISSN (P) 2454-0663

Authenticated broadcast and flooding

A lot of protocols require nodes to broadcast HELLO messages to their neighbors. These messages should be authenticated and impossible to spoof. Authenticated broadcast proposed for use in a more conventional setting either use digital signatures and/or have packet overhead that well exceed the length of the typical sensor network packet. µTESLA is a protocol for efficient, authenticated broadcast and flooding that uses only symmetric key cryptography and requires minimal packet overhead. Replay is prevented because messages authenticated with previously disclosed keys are ignored.

II CONCLUSION AND FUTURE WORK

Secure routing is key to the acceptance and use of sensing element networks for several applications. Link layer cryptography and authentication approach is also a smart initial approximation for defense. Sensing element network routing protocols should be designed with security in mind. Link-layer cryptography and authentication are multipath routing, biometric identification, bifocal link verification and attested broadcast will keep the sensing element network routing protocols against outsiders, fake routing data, Sybil attacks, howdy floods, and acknowledgment spoofing, and it's possible to enlarge existing protocols with these mechanisms. Depression attacks and wormholes masquerade major challenges to secure routing protocol style and it's unlikely there exist effective countermeasures against these attacks that may be helpful once the planning of a protocol has finished. It's important to style, routing protocols within which these attacks are vacuous or ineffective. Geographic routing protocols are one category of protocols that holds promise. A limitation of building a multi-hop routing topology around a hard and fast set of base stations is that those nodes among one or 2 hops of the bottom stations are notably enticing for compromise. If a major variety of those nodes are compromised, then all is lost. We tend to believe it's still associate open drawback to style a wireless sensing element network routing protocol that satisfies each the planned security goals and bring home the bacon the facility savings of state-of the-art sensing element network routing protocols.

That is as a result of such protocols usually believe organizations and on nodes and even the bottom station having solely native data. In such paradigm wherever the system isn't globally proverbial it's terribly exhausting to realize security. To get world information is commonly a task too pricey for sensing element networks. Discuss the progressive highlight the provide directions for future work.

REFERENCES

[1] J.N. Al-Karaki and A.E. Kamal, “Routing techniques in wireless sensor networks: a survey”. IEEE Wireless Communications, 11(6):6–28, 2004.

[2] Pieter Beyens, Maarten Peeters, Kris Steenhaut, and Ann Nowe, “Routing with compression in wireless sensor networks: a q-learning approach”, In Fifth European Workshop on Adaptive Agents and Multi-Agent Systems, pages 575–578, Washington, DC, USA, 2005. IEEE Computer Society.

ISSN (O) 2454-9665
ISSN (P) 2454-0663

[3] Long Gan, Jiming Liu, and Xiaolong Jin. "Agent-based energy efficient routing in sensor networks", In AAMAS '04: Proceedings of the Third International Joint Conference on Autonomous Agents and Multiagent Systems, pages 472–479, Washington, DC, USA, 2004. IEEE Computer Society.

[4] W. Heinzelman, A. Chandrakasan, and H. Balakrishnan, "An application-specific protocol architecture for wireless microsensor networks", IEEE Transactions on Wireless Communications, 1(4):660–670, October 2002.

[5] Y. Hu, A. Perrig, and D. Johnson, "Wormhole detection in wireless ad hoc networks", Technical report, 2002.

[6] Y.C. Hu, A. Perrig, and D.B. Johnson, "Wormhole detection in wireless ad hoc networks", Tech. Rep. TR01-384, Department of Computer Science, Rice University, June 2002.

[7] C. Karlof and D. Wagner. "Secure routing in wireless sensor networks: Attacks and countermeasures", In First IEEE International Workshop on Sensor Network Protocols and Applications, pages 113–127, May 2003.

[8] Arati Manjeshwar and Dharma P. Agrawal, "Teen: Arouting protocol for enhanced efficiency in wireless sensor networks" In IPDPS '01: Proceedings of the 15th International Parallel & Distributed Processing Symposium, page 189, Washington, DC, USA, 2001. IEEE Computer Society.

[9] A. Perrig, R. Szewczyk, J.D. Tygar, V. Wen, and D.E. Culler. Spins, "security protocols for sensor networks", Wirel. Netw., 8(5):521–534, 2002.

[10] J.P. Walters, Z. Liang, W. Shi, and V. Chaudhary, "Wireless sensor network security: A survey", 2006

[11] Karlof, C. and Wagner, D, "Secure routing in wireless sensor networks: Attacks and countermeasures", In Proceedings of the 1st IEEE International Workshop on Sensor Network Protocols and Applications Anchorage, AK, May 11, 2003.