ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 7, Issue 5, May 2019

A Survey on Packet Droppers and Modifier Using Wireless Sensor Network

Raghuram A S [1]

Assistant Professor, Department of Computer Engineering, ATME College of Engineering, Mysore, India[1]

ABSTRACT: In a wireless sensor network, sensor nodes monitor the environment, detect events of interest, produce data and collaborate in forwarding the data toward a sink. Because of the ease of deployment, the low cost of sensor nodes and the capability of self-organization, a sensor network is often deployed in an unattended and hostile environment to perform the monitoring and data collection tasks. When it is deployed in such an environment, it lacks physical protection and is subject to node compromise. After compromising one or multiple sensor nodes, an adversary may launch various attacks to disrupt the in-network communication. Among these attacks, two common ones are dropping packets and modifying packets, i.e., compromised nodes drop or modify the packets that they are supposed to forward.

KEYWORDS: compromised nodes, wireless sensor network

I. INTRODUCTION

In computer networking, a **packet drop attack** or **black hole attack** is a type of denial-of-service attack in which a router that is supposed to relay packets instead discards them. This usually occurs from a router becoming compromised from a number of different causes.

A **wireless sensor network (WSN)** of spatially distributed autonomous sensors to *monitor* physical or environmental conditions, such as temperature, sound, pressure, etc. and to cooperatively pass their data through the network to a main location. The more modern networks are bi-directional, also enabling *control* of sensor activity. The development of wireless sensor networks was motivated by military applications such as battlefield surveillance; today such networks are used in many industrial and consumer applications, such as industrial process monitoring and control, machine health monitoring, and so on.

Keywords:black hole attack, wireless sensor network

II. RELATED WORK

1. Secure Routing in Wireless Sensor Networks: Attacks and Countermeasures

Security goals for routing in sensor networks show how attacks against ad hoc and peer-to-peer networks can be adapted into powerful attacks against sensor networks, introduce two classes of novel attacks against sensor networks sinkholes and HELLO floods, and analyze the security of the entire major sensor network routing protocols. We describe crippling attacks against all of them and suggest countermeasures and design considerations.

We use the term sensor network to refer to a heterogeneous system combining tiny sensors and actuators with general purpose computing elements. Sensor networks may consist of hundreds or thousands of low-power, low-cost nodes, possibly mobile but more likely at fixed locations, deployed en masse to monitor and affect the environment.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 7, Issue 5, May 2019

We target the Berkeley TinyOS sensor platform in our work. Because this environment is so radically different from any we had previously encountered, we feel it is instructive to give some background on the capabilities of the Berkeley TinyOS platform.

In order to reduce the total number of messages sent and thus save energy, sensor readings from multiple nodes may be processed at one of many possible aggregation points. An aggregation point collects sensor readings from surrounding nodes and forwards a single message representing an aggregate of the values. Aggregation points are typically regular sensor nodes, and their selection is not necessarily static. Aggregation points could be chosen dynamically for each query or event.

Some of the attacks against proposed sensor networks routing protocols are:

- TinyOS beaconing
- Directed diffusion and its multipath variant
- Geographic routing (GPSR, GEAR)
- Minimum cost forwarding
- Clustering based protocols (LEACH, TEEN,PEGASIS)
- Rumor routing Energy conserving topology maintenance(SPAN, GAF, CEC, AFECA)

Secure routing is vital to the acceptance and use of sensor networks for many applications, but we have demonstrated that currently proposed routing protocols for these networks are insecure. Link layer encryption and authentication mechanisms may be a reasonable first approximation for defense against mote-class outsiders, but cryptography is not enough to defend against laptop-class adversaries and insiders: careful protocol design is needed as well.

2. Detecting False Data in Wireless Sensor Network using Efficient Becan Scheme

Wireless sensor networks range from smart applications such as traffic monitoring to critical military applications such as measuring levels of gas concentration in battle fields, security in sensor networks becomes a prime concern. In sensitive applications, it becomes imperative to continuously monitor the transient state of the system rather than steady state observations and take requisite preventive and corrective actions. Networks are prone to be attacked by adversaries who intend to disrupt the functioning of the system by compromising the sensor nodes and injecting false data into the network. We use a novel bandwidth-efficient cooperative authentication (BECAN) scheme for filtering injected false data based on Bloom Filter.

Wireless sensor network is a collection of nodes organized into a cooperative network. Each node consists of processing capability with one or more microcontrollers, CPUs or DSP chips and may contain multiple types of memory or flash memory which holds program or data. Each node has a RF transceiver usually with a single Omni-directional antenna, and a power source such as batteries and solar cells, and accommodates various sensors and actuators

WSN technology has many applications including various environmental monitoring. A primitive objective of WSNs is to answer queries by gathering sensory data from the deployed sensors. The mechanism of using Bloom Filter for filtering injected false data in wireless sensor networks is proposed and it is called as bandwidth-efficient cooperative authentication (BECAN) scheme.

This scheme achieves high filtering and reliability when comparing with the previously reported mechanisms. It also prevents the gangs injecting false data attack from mobile compromised sensor nodes using Ad hoc on-demand distance vector (AODV) routing protocol.

A different BECAN scheme is proposed for filtering the injected false data based on Bloom filter. The BECAN scheme can achieve better en-routing filtering probability and improved reliability with multi-reports. The performance of the packet delivery ratio, end-to-end latency and throughput of the proposed system are achieved in the simulation experiments. BECAN can also be applied on other distributed authentication scenario since it prevents unauthorized access through injecting false data attack from mobile compromised sensor nodes through routing protocols.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 7, Issue 5, May 2019

3. An Acknowledgment-Based Approach for the Detection of Routing Misbehaviour in MANETs

Routing misbehaviour is that some selfish nodes will participate in the route discovery and maintenance processes but refuses to forward data packets. We propose the 2ACK scheme that serves as an add-on technique for routing schemes to detect routing misbehaviour and to mitigate their adverse effect. The main idea of the 2ACK scheme is to send two-hop acknowledgment packets in the opposite direction of the routing path. In order to reduce additional routing overhead, only a fraction of the received data packets are acknowledged in the 2ACK scheme. Analytical and simulation results are presented to evaluate the performance of the proposed scheme.
A Mobile Ad Hoc Network (MANET) is a collection of mobile nodes (hosts) which communicate with each other via wireless links either directly or relying on other nodes as routers. The operation of MANETs does not depend on preexisting infrastructure or base stations. Network nodes in MANETs are free to move randomly. Therefore, the network topology of a MANET may change rapidly and unpredictably.The structure of a MANET may vary from a small, static network that is highly power-constrained to a large-scale, mobile, highly dynamic network. There are two types of MANETs: closed and open.
Several techniques have been proposed to detect and alleviate the effects of such selfish nodes in MANETs. The two techniques were introduced, namely,

- watchdogand
- pathrater

The watchdog technique identifies them is behaving nodes by overhearing on the wireless medium. The pathrater technique allows nodes to avoid the use of the misbehaving nodes in any future route selections.
We propose the 2ACK scheme to mitigate the adverse effects of misbehaving nodes. The basic idea of the 2ACK scheme is that, when a node forwards a data packet successfully over the next hop, the destination node of the next-hop link will send back a special two-hop acknowledgment called 2ACK to indicate that the data packet has been received successfully. A selfish node does not perform the packet forwarding function for data packets unrelated to it. However, it operates normally in the Route Discovery and the Route Maintenance phases of the DSR protocol.
We have investigated the performance degradation caused by such selfish (misbehaving) nodes in MANETs. We have proposed and evaluated a technique, termed 2ACK, to detect and mitigate the effect of such routing misbehavior. The 2ACK technique is based on a simple 2-hop acknowledgment packet that is sent back by the receiver of the next-hop link. Compared with other approaches to combat the problem, such as the overhearing technique, the 2ACK scheme overcomes several problems including ambiguous collisions, receiver collisions, and limited transmission powers.
The 2ACK scheme can be used as an add-on technique to routing protocols such as DSR in MANETs. In our future work, we will investigate how to add the 2ACK scheme to other types of routing schemes and open networks. Theoretical analysis of the performance gain of the 2ACK scheme is of interest as well.

4.The Selective Forwarding Attack in Sensor Networks: Detections and Countermeasures

Sensor networks are becoming closer towards wide-spread deployment so security issues become a vital concern. Selective forwarding attack is one of the harmful attacks against sensor networks and can affect the whole sensor network communication. The variety of defence approaches against selective forwarding attack is overwhelming. This paper also classifies proposed schemes according to their nature and defence. Nature of scheme classifies into Distributed and Centralized. Defence of scheme classifies into detection and prevention.
Wireless Sensor Networks are modernizing the way the people interact with the physical world. They comprise of small sensor nodes which have many capabilities such as sensing, monitoring, computation and wireless communications. They are deployed in large amounts to collect data from the environment, perform local processing and communicate their results. In this paper, we investigate the Selective Forwarding Attack and its variants, which is very simple to implement but difficult to detect. In selective forwarding attack the malicious node works as a normal node but refuses to forward certain selected packets and simply drop them. So, due to this nature, the selective

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 7, Issue 5, May 2019

forwarding attack is very harmful for mission critical applications and can damage the whole network communication, making the network useless.

Some of Multi-hop Routing Protocols are:

- TinyOS beaconing
- Directed diffusion and its Multipath Variant
- Geographic Routing (GPSR, GEAR)
- Minimum Cost Forwarding
- Clustering based protocols (LEACH, TEEN, PEGASIS)
- Rumor Routing
- PSFQ
- DSR

Schemes against Selective Forwarding Detection and Countermeasures are:

1. Secure routing in wireless sensor networks: attacks and countermeasures.
2. Detecting Selective Forwarding Attacks in Wireless Sensor Networks
3. CHEMAS: Identify suspect nodes in selective forwarding attacks
4. Detecting Selective Forwarding Attacks in Wireless Sensor Networks using SVMs
5. An Efficient Countermeasure to the Selective Forwarding Attack in Wireless Sensor Networks
6. Towards Intrusion Detection in Wireless Sensor Networks
7. Fuzzy-Based Reliable Data Delivery for Countering Selective Forwarding in Sensor Networks
8. Detecting Selective Forwarding Attacks in Wireless Sensor Networks Using Two-hops Neighbor Knowledge
9. CADE: Cumulative Acknowledgement based Detection of Selective Forwarding Attacks in Wireless Sensor Networks
10. Detection of Selective Forwarding Attacks in Heterogeneous Sensor Networks

One more thing that the authors doing research in this area must consider is that their proposed schemes must be capable of perceiving the true causes of packet dropping that is it can distinguish that packets are dropping either due to congestion or by a malicious node. Also, it is of the essence that the schemes or techniques proposed in future should be enough competent so that they can both detect and prevent the selective forwarding attack as an attack detection scheme itself cannot be an ultimate solution and prevention may be safer than relying on detection. Winding up, almost all existing schemes have drawbacks hence; a very vigilant, efficient, economical and node cooperation based defensive mechanism is needed to counter the selective forwarding attack.

5. Secure and Data Aggregation in Wireless Sensor Networks

Data aggregation is implemented in wireless sensor networks to reduce data redundancy and to summarize relevant and necessary information without requiring all pieces of the data. The benefit of data aggregation can be maximized by implementing it at every data aggregator on the path to the base station.

Data congeniality requires sensor nodes to encrypt their data prior to transmission. Moreover, once data is encrypted by a sensor node, it should be decrypted at the base station to maintain end-to-end security. This makes the implementation of data aggregation very difficult because data aggregation algorithms require encrypted data to be decrypted. Consequently, data aggregation and secure communication have conflicts in their implementation. In order to overcome this problem shared key signature is proposed as an encryption technique.

A wireless sensor node is equipped with sensing and computing devices, radio transceivers and power components. The individual nodes in a wireless sensor network (WSN) are inherently resource constrained: they have limited processing speed, storage capacity, and 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 onboard sensors start collecting information of interest

A number of mechanisms called aggregation algorithms are suggested in order to omit the redundant data. Aggregation algorithms, after receiving data from several sensors, process data and omit the redundancy and send the result of aggregation to the sink. Due to the reduction in data volume, these algorithms decrease the energy consumption.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 7, Issue 5, May 2019

Therefore the networks which perform aggregation have more life time and draw more attention. In addition to mentioned improvements, aggregation decreases collision and retransmission delay
Scheme for data aggregations are:

1. **A RCDA Scheme for Homogeneous WSN (RCDA-Homo)**
2. **A Rcda Scheme For Heterogeneous Wsn**

Security is becoming a major concern for energy constrained wireless sensor network because of the broad security-critical applications of WSNs. Thus, security in WSNs has attracted a lot of attention in the recent years. Recoverable concealed data aggregation schemes for homogeneous/heterogeneous WSNs have been proposed. A special feature is that the base station can securely recover all sensing data rather than aggregated results, but the transmission overhead is still acceptable. Moreover, aggregate signature scheme to ensure data authenticity and integrity in the design has been integrated. Even though signatures bring additional costs, the proposed schemes are still affordable for WSNs after evaluation. Network security for WSNs is still a very fruitful research direction to be further explored.
of extending DSDV to behave like a path-vector routing protocol, allowing the source address of each advertisement to be more readily authenticated in our future work.

III.CONCLUSION

Packet dropping and modification are common attacks that can be launched by an adversary to disrupt communication in wireless multi hop sensor networks. Many schemes have been proposed to mitigate or tolerate such attacks, but very few can effectively and efficiently identify the intruders. To address this problem, we propose a simple yet effective scheme, which can identify misbehaving forwarders that drop or modify packets. These countermeasures can tolerate or mitigate the packet dropping and modification attacks, but the intruders are still there and can continue attacking the network without being caught.

Many methodology Proposed to get a simple yet effective scheme to catch both packet droppers and modifiers by implementing an application to identify nodes that are droppers/modifiers for sure or are suspicious droppers/modifiers. The system can be used in all the wireless networks to have a secured network information exchange and assure the delivery of information to the destination.

REFERENCES

[1] Chris Karlof, David Wagner, "Secure Routing in Wireless Sensor Networks: Attacks and Countermeasures" Computer, vol. 36, no. 10, pp. 103-105, Oct. 2003.
[2] S. Sajithabanu , M. Durairaj, "Detecting False Data in Wireless Sensor Network using Efficient Becan Scheme"*International Journal of Computer Applications (0975 – 8887) Volume 43– No.18, April 2012*
[3] Kejun Liu, Jing Deng, Pramod K. Varshney, and KashyapBalakrishnan,"An Acknowledgment-Based Approach for the Detection of Routing Misbehaviour in MANETs "*IEEE Transactions on Mobile Computing, vol. 6, no. 5, pp. 536-550, May 2007.*
[4] WazirZadaKhana, Yang Xiangb, Mohammed Y Aalsalema, QuratulainArshada," The Selective Forwarding Attack in Sensor Networks: Detections and Countermeasures" vol .2, no. 12,pp. 33-44, April 2012.
[5] R.MohanaSundari, Mrs.P.R.Vijayalakshmi" Secure and Data Aggregation in Wireless Sensor Networks"
International Journal of Advanced Engineering Applications, Vol.4, Iss.1, pp.32-36 (2011).
[6] Yih-Chun Hu a, David B. Johnson b, Adrian Perrig,"SEAD: secure efficient distance vector routing for mobile wireless ad hoc networks" vol. 1,no. 18,pp. 175–192,(2003).
[7] sencunzhu, sanjeevsetia, sushiljajodia, pengning, " Interleaved hop-by-hop authentication against false data injection attacks in sensor networks" IEEE Symp. Security and Privacy, 2004.
[8] Fan Ye, HaiyunLuo, Songwu Lu, *Member, IEEE, and Lixia Zhang, Senior Member, IEEE.*" Statistical en-route filtering of injected false data in sensor networks" IEEE journal on selected areas in communications, vol. 23, no. 4, April 2005.
[9] Xin Zhang, Abhishek Jain, Adrian Perrig, " Packet-dropping Adversary Identification for Data Plane Security"vol.5,no. 9-12, December 2008.
[10] Rosa Mavropodi , Panayiotis Kotzanikolaou, Christos Douligeris, " SecMR – a secure multipath routing protocol for ad hoc networks" science direct, Ad Hoc Networks 5 (2007) 87–99.
[11] H.Chan and A. Perrig, "Security and Privacy in Sensor Networks," IEEE Computer, October 2003.
[12] V. Bhuse, A. Gupta, and L. Lilien, "Dpdsn: Detection of packet-dropping attacks for wireless sensor networks," In the Trusted Internet Workshop, International Conference on High Performance Computing, December 2005.