RESEARCHERID
THOMSON REUTERS

[Acharya* 5(6): June, 2018] ISSN 2349-4506
Impact Factor: 3.799

Global Journal of Engineering Science and Research Management

A CRITICAL SURVEY ON DETECTION OF MALICIOUS NODES AND FALSE REPORTING THROUGH ADAPTIVE ACKNOWLEDGMENT (EAACK) FOR WSN

Sachin Acharya T*, Shobhan Kumar
* Computer Science and Engineering Dept, Sahyadri College of Engineering and Management Mangalore

DOI: 10.5281/zenodo.1286780

KEYWORDS: WSN, Security attacks in WSN, Enhanced Adaptive Acknowledgement, EAACK, False Misbehavior Reporting, and Misbehavior Report Authentication.

ABSTRACT
WSNs are the temporary networks which are dynamic and self-maintainable. As being dynamic in nature and without any fixed infrastructure, the security becomes a great concern in WSNs. There are different types of security attacks like black hole, worm hole and grey hole but in this paper we are only focusing on the detection of malicious nodes and false reporting. We propose and implement a new intrusion-detection system named Enhanced Adaptive Acknowledgment (EAACK) specially designed for WSNs. Compared to contemporary approaches, EAACK demonstrates higher malicious behavior detection rates in certain circumstances while does not greatly affect the network performances.

INTRODUCTION
Wireless sensor network is a group of specialized transducers that are deployed in particular environment to gather information. Wireless sensor network is an advanced technology with their limited energy, processing and transmission capabilities. WSN have gained popularity due to their usage in various applications in impractical environments. A typical WSN consists of battery-powered sensor nodes with data acquisition, processing and transmitting components. The main challenge for sensor networks consists of two aspects. First, sensor nodes have some resource constraints. Second, in several applications sensor nodes are randomly deployed to monitor particular environment [3]. An application that uses sensor networks are distributed in nature and basically route messages using wireless communication medium. Wireless communication medium is inherently insecure and sensor nodes have low computational power processors, low memory, and runs on battery. In addition, sensor nodes are likely be deployed in open, physically impractical, or hostile environments where sensor nodes can be easily compromised by the attackers.

A typical sensor node consists of three subsystems. *Sensing subsystem* for data acquisition, *processing subsystem* for processing gathered information, and *Communication subsystem* for the transmission of gathered information. Finally, the three subsystems of sensor nodes run on the energy provided by underlying battery. Though sensor nodes are deployed in impractical environments, security requirements is to be provided such as integrity, confidentiality, and availability so on.

RELATED WORK
The nodes in WSNs assume that other nodes always cooperate with each other in data transmission. This assumption leaves the attackers to cause significant impact on the network with just one or two compromised nodes. To address this problem, Intrusion Detection Systems should be added to enhance the security level of WSNs. If WSN can detect the attackers as soon as they enter the network, we will be able to completely eliminate the potential damages caused by compromised nodes. In this paper, we discuss some of the security schemes which are being used so far.

Watchdog Marti *et al.* [6] proposed the Watchdog scheme. It improves the throughput of network with the presence of malicious nodes. The Watchdog scheme consists of two parts i.e 'Watchdog' and 'Pathrater'. Watchdog serves as an Intrusion detection system for WSNs. It is responsible to detect malicious node misbehavior in the network. It detects the malicious misbehaviors by listening to its next hop's transmission. If a Watchdog node overhears that its next node fails to forward the packet within a certain period of time, it increases its failure counter. Whenever a node's failure counter exceeds a predefined threshold, the Watchdog node reports

it as misbehaving. In this case, the Pathrater cooperates with the routing protocols to avoid the reported nodes in future transmission. The Watchdog scheme fails to detect malicious misbehaviors with the presence of the following: 1) ambiguous collisions; 2) receiver collisions; 3) limited transmission power; 4) false misbehavior report; 5) collusion; 6) partial dropping.

TWOACK To overcome the weaknesses of the Watchdog scheme, a new scheme named TWOACK was proposed by Liu *et al.* [7] Aiming to resolve the receiver collision and limited transmission power problems of Watchdog, TWOACK detects misbehaving links by acknowledging every data packet transmitted over every three consecutive nodes along the path from the source to the destination. Upon retrieval of a packet, each node along the route is required to send back an acknowledgment packet to the node that is two hops away from it down the route. TWOACK is required to work on routing protocols such as Dynamic Source Routing (DSR) [9]. The receiver collision and limited transmission power problems posed by Watchdog are solved by this scheme. But the acknowledgment process required in every packet transmission process increased the network traffic. Due to the limited battery power nature of WSNs, such redundant transmission process can degrade the life span of the entire network

Sheltami*et al.* [10] proposed a new scheme called AACK. Similar to TWOACK, AACK is an acknowledgment-based network layer scheme which is a combination of a scheme called TWOACK and an end-to-end acknowledgment scheme called ACKnowledge (ACK). Compared to TWOACK, AACK significantly reduced network overhead while still capable of maintaining or even surpassing the same network throughput. Within a predefined time period, if the source node receives this ACK acknowledgment packet, then the packet transmission from source node to destination node is successful. Otherwise, the source node will switch to TWOACK scheme by sending out a ACK packet. This scheme reduces the network overhead, but both TWOACK and AACK fails to detect the malicious nodes and false misbehavior reporting.

METHODOLOGY

Security Requirement The security requirements [1] for a wireless sensor network can be classified into following ways:

- **Integrity:** The data in transmission between sensor nodes can be altered by the adversaries. Data integrity should be provided to ensure that information is not altered in transmission.
- **Authentication:** As WSN communicates sensed data, the sender/receiver needs to authenticate each other while exchanging the control information.
- **Confidentiality:** Applications like military, secret applications and key exchanges need the confidentiality of data. Confidentiality can be provided through the use of cryptographic techniques on the data.
- **Availability:** Sensor nodes always run on battery power, so due to some extra processing or communication overhead it may become unavailable. So it's highly important to maintain the availability of the sensor nodes through some energy conservation schemes.
- **Data Freshness:** In addition to data confidentiality, data integrity and availability, we also need to ensure the freshness of each transmitted message that no old messages are replayed by adding time stamp to the packet

Security attacks Attacks on the sensor networks can be classified [2] as following ways:

- **Interruption** is a class of attack on WSN where the availability of the sensor nodes is damaged. It includes problems such as malicious content insertion, capturing the nodes, corrupting messages etc.
- **Interception** is a class of attack on WSN where the confidentiality of data that's being transmitted over the network is disclosed. It includes unauthorized access to sensor node or data within it.
- **Modification** is a class of attack on WSN where the integrity of data that's being transmitted over the network is modified. It includes the modification of the data packets or causing denial of service attack.
- **Fabrication** is a class of attack on WSN where the authentication for the transfer of control information is altered. In this sort of attacks an intruder injects false data and gains the trustworthiness.

These are all the different classes of attacks that may occur in sensor network. This classes of attacks can be rectified by using some acknowledgement schemes that ensure about the attacks on which preventive actions can be taken. But traditional acknowledgement schemes are volatile for the attacks that are explained below such as black hole and grey hole attacks.

A. Black Hole Attack: A black hole attack is a kind of attack in WSN where a malicious node in the sensor network makes use of the routing information and represents itself has the shortest path to the destination node in the sensor network. After representing itself as a shortest path to destination node, the malicious node receives routing packets and does not forward packets to its neighbor nodes. This kind of malicious node is called *black hole* [4]. After the creation of this black hole in sensor network the source node sends out its data packets to the black hole believing that it's the shortest path to destination node. Thus the black hole receives all sent packets from the source node and behalf of forwarding those data packets to the destination it will simply discard those packets. So the data packets obtained by the black hole node will not arrive at the destination node.

B. Grey Hole Attack: This attack is sometimes also called as selective forwarding[5]. The grey hole attack is a kind of attack in WSN where a malicious node in the sensor network tries to stop the data packets that are passing through it in a sensor network by refusing to forward the data packets or dropping the data packets passing through them. In this grey hole attack, the malicious node can selectively drops the data packets coming from particular sensor node.In this sort of attacks the malicious nodes may also behave like black hole and refuses to forward the data packets passing through them.

As explained above the black hole and grey hole attacks are two severe attacks on WSN with passive nature. Due to their passive nature, the present acknowledgements schemes are vulnerable to this kind of attacks on WSN. The present acknowledgement schemes are explained in next section with their related work in field of WSN.

PROPOSED SCHEME

In order to overcome the drawbacks of the above discussed schemes, the Enhanced Adaptive Acknowledgement scheme (EAACK) was introduced. EAACK consists of three major parts, namely, ACK, Secure ACK (S-ACK), and misbehavior report authentication (MRA)[13].

A. ACK

ACK is basically an end-to-end acknowledgment scheme. It acts as a part of the hybrid scheme in EAACK, aiming to reduce network overhead when no network misbehavior is detected. If the ACK packet doesn't reach the source in predefined period of time then ACK scheme will be adopted for the network.

B. S-ACK

The S-ACK scheme is an improved version of the TWOACK. Here every three consecutive nodes work in a group to detect misbehaving nodes. For every three consecutive nodes in the route, the third node is required to send an S-ACK acknowledgment packet to the first node. The intention of introducing S-ACK mode is to detect misbehaving nodes in the presence of receiver collision or limited transmission power.

C. MRA

The false misbehavior report can be generated by malicious attackers to falsely report innocent nodes as malicious. The Misbehavior Report Authentication scheme (MRA) is designed to detect misbehaving nodes with the presence of false misbehavior report. This scheme authenticates whether the destination node has received the reported missing packet through a different route. To initiate the MRA mode, the source node first searches its local cache and finds out an alternative route to the destination node. Then using the new route, the source sends out a MRA packet to the destination. If the MRA packet is matches with the data packet at the destination then false misbehavior is reported and the malicious node responsible for it is ignored in the further transmission.

CONCLUSION

In this research paper, we have proposed a novel technique named EAACK protocol to overcome the network security issues in WSN. This scheme has positive results against the drawbacks of Watchdog, TWOACK, and AACK in the cases of receiver collision, limited transmission power and false misbehavior reporting. The MRA

protocol also helps to overcome false misbehavior reporting and helps in the detection of malicious nodes within the WSN. These nodes can be avoided in further transmission in order to maintain the network performance.

REFERENCES

1. ZoranS.Bojkovic, Bojan M. Bakmaz, and Miodrag R. Bakmaz, "Security Issues in Wireless Sensor Networks", International Journal Of Communication, Issue 1, Volume 2, 2008
2. Romer, K., Mattern, F. & Zurich, E.,"The Design Space of Wireless Sensor Networks,"IEEE Wireless Communication.2004
3. Shio Kumar, M P Singh , and D K Singh, " Routing Protocols In Wireless Sensor Networks- A Survey"
4. M. Al-Shurman, S. M. Woo, S. Park, "*Black Hole Attack in Mobile Ad-Hoc Networks*", ACMSE'04, Huntville, AL, USA, April 2-3,2004. International Journal of Computer Science & Engineering Survey (IJCSES) Volume 1,November 2010
5. C. Karlof, D.Wagner, "Secure routing in wireless sensor networks: Attacks and countermeasures,Special Issue on Sensor Network Applications and Protocols", vol 1 (2-3), 2003,pp.1293 –1303
6. S. Marti, T. J. Giuli, K. Lai, and M. Baker, "Mitigating routing misbehaviour in mobile ad hoc networks," in *Proc. 6th Annu.Int. Conf. Mobile Comput.Netw.*, Boston, MA, 2000, pp. 255–265.
7. K. Liu, J. Deng, P. K. Varshney, and K. Balakrishnan, "An acknowledgment-based approach for the detection of routing misbehaviour in MANETs," *IEEE Trans. Mobile Comput.*, vol. 6, no. 5,pp. 536–550, May 2007.
8. A. Menezes, P. van Oorschot, and S. Vanstone, *Handbook of Applied Cryptography*. Boca Raton, FL: CRC, 1996, T-37.
9. D. Johnson and D. Maltz, "Dynamic Source Routing in *ad hoc* wireless networks," in *Mobile Computing*. Norwell, MA: Kluwer, 1996, ch. 5,pp. 153–181.
10. T. Sheltami, A. Al-Roubaiey, E. Shakshuki, and A. Mahmoud, "Video transmission enhancement in presence ofmisbehaving nodes inMANETs," *Int. J. Multimedia Syst.*, vol. 15, no. 5, pp. 273–282, Oct. 2009.
11. R. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," *Commun. ACM*, vol. 21, no. 2, pp. 120–126, Feb. 1983.
12. Nat. Inst. Std. Technol., Digital Signature Standard (DSS) Federal Information Processing Standards Publication, Gaithersburg, MD, 2009, Digital Signature Standard (DSS).
13. EAACK—A Secure Intrusion-Detection System for MANETs Elhadi M. Shakshuki, *Senior Member, IEEE,* Nan Kang, and Tarek R. Sheltami, *Member, IEEE,* IEEE