A Novel Algorithm for Detecting Sinkhole Attacks in WSNs

Maliheh Bahekmat, Mohammad Hossein Yaghmaee, Ashraf Sadat Heydari Yazdi, and Sanaz Sadeghi

***Abstract*—Nowadays with the wide range of applications in wireless sensor networks, there is an increasing need for security of these networks. These networks have been subjected to numerous attacks among which Sinkhole attack is one of the notable ones. In Sinkhole attack, sometimes the adversary node poses itself as a fake base station (BS) and receives all data of the network. It prevents data from reaching the main BS, or changes the received data and then transfers them to the main BS. In this paper, we present an efficient algorithm in terms of energy consumption. In the proposed algorithm, when a node desires to send data to the BS, it firstly sends a control packet directly to the main BS. Then it begins to send data packets to the BS in form of hop by hop routing. When the data packet arrives at the BS, some of its control fields are compared with the same ones of the original control packet. If any changes have been made to these control fields of the data packet, it shows that there is a malicious node; the BS detects it using the proposed strategy. The performance of the proposed method has been evaluated and compared with that of Ngai's algorithm. The simulation results indicate that the proposed algorithm is more efficient than it.**

***Index Terms*—Wireless sensor networks, sinkhole attack, wormhole, base station, detection.**

I. Introduction

Wireless sensor network consists of several sensor nodes that collect data in inaccessible areas and send them to the BS after initial processing [1]. Nowadays, with respect to the increasing number of applications such as: environmental, medical, military, industrial applications, etc, designing efficient security mechanisms considering the type of the applications is obviously needed. Sensor networks face restrictions in implementation of security patterns which are used in traditional networks. For example, digital signature algorithm cannot be implemented in these networks because of the limited amount of memory and low processing capabilities. Therefore, we need to utilize algorithms to obviate the security requirements of these networks in a way that it doesn't draw excessive overhead on the sensor node resources [2]. Security objectives of wireless sensor networks include [2]:

• **Data confidentiality**: encrypting data to render it imperceptible to the unauthorized sensors is the first security requirement of the sensor network [3].

• **Data accuracy**: these algorithms have been designed to ensure that the data have not been manipulated en route by other sensor nodes. In the most preliminary approach, MAC is calculated from the message and forwarded with the original message.

• **Data freshness**: it prevents resending old data from the adversary sensor nodes and ensures that the data received by the receivers is fresh [4].

• **Resistance and fault tolerance**: sensor networks need to be resistant against numerous attacks, and if a successful attack have been made, its impact should be local without disrupting the entire network.

The structure of the current paper is organized as follows. In section 2, we explore variety of common attacks to sensor networks and discuss some detection methods. In the third section, we investigate the details of the proposed method.

Simulation results are given in section 4. Finally, section 5 concludes the paper.

II. Related Works

The attacks to sensor networks can be considered from two perspectives. One of them deals with the attacks made against the security mechanism of the network and another one copes with the attacks made to the ordinary operation of the network such as routing, data collection, etc. Furthermore, these attacks, based on the capacities of the adversary, can be divided into two categories, named Mote and Laptop. The latter sensors have more capacities and fewer restrictions in terms of resources, while the former, with respect to the functionality and the level of hardware equipment, resembles the ordinary sensors in the network. In the sensor networks, there are possible attacks such as Hell Flood, Sinkhole, Sybil, DOS and Wormhole [5].

In the Sinkhole attack, the adversary's goal is to lure nearly all the traffic from a particular area through a compromised node, creating a metaphorical Sinkhole with the adversary at the center. Sinkhole attacks typically work by making a compromised node look especially attractive to surrounding nodes with respect to the routing algorithm. For instance, an adversary could spoof or replay an advertisement for an extremely high quality route to a BS. Due to either the real or imagined high quality route through the compromised node, it is likely each neighboring node of the adversary will forward packets destined for a BS through the adversary, and also propagate the attractiveness of the route to its neighbors. Effectively, the adversary creates a large "sphere of influence" [6], attracting all traffic destined for a BS from nodes several hops away from the compromised node. The possibility of using the radio signal strength to detect compromised nodes was studied in [7]. This method assumes that each node has a unique id and can know the location

Manuscript received March 25, 2012; revised May 10, 2012.

Maliheh Bahekmat, Ashraf Sadat Heydari Yazdi and Sanaz Sadeghi are with the Department of computer engineering, Ferdowsi University of Mashhad, Iran (e-mail: ma.bahekmat@um.ac.ir).

Mohammad Hossein Yaghmaee was with the Lane Department of Computer Science and Electrical Engineering, West Virginia University, Morgantown, USA.

information using positioning system like GPS. The geographical location information and id are included in each message and the messages are designed to be tamper-resistant. Each node monitors all the transmissions it can hear, and obtains two values for every transmission: the expected signal strength, and the actual signal strength. However, this method incurs a large overhead, and it does not take into account that signal strengths might change due to other environmental or operating factors such as decreasing transmission power of a node over the time. Onat and Miri developed an algorithm to detect compromised nodes by inspecting the stable neighbor information [8]. With the assumption that every node in the network has the ability to distinctively identify its neighbors, two parameters are defined to characterize the neighbors based on the packet arrival rate and the receive power. If these parameters exceed certain thresholds, an intruder is detected and an alert is generated. If a node hears the intruder alerts from more than a preset number of its neighbors, it flags the suspected node as a compromised node. One restriction of this method is that it does not allow new nodes to join the network after the initial deployment. In [9], the authors propose a detection algorithm for Sinkhole attack. In Sinkhole attack, malicious nodes pretend to have the shortest paths to the BS to trick other nodes into forwarding messages to them. This causes an increase in network traffic in the areas surrounding the malicious nodes. To detect a single malicious node, the BS monitors the data consistency among the nodes. If one node's behavioral anomaly exceeds a predetermined threshold, then this node is considered suspicious. After analyzing the routing pattern, the BS could identify the malicious node. To further solve the problem that some malicious nodes could collude to avoid being detected; this algorithm uses additional measures such as key establishment and path redundancy. However, this approach is only effective for static networks. In [10], the authors propose a localized approach to detect compromised nodes. All the sensor nodes are divided into multiple groups. A Data Transmission Quality (DTQ) function is defined to measure the communication quality of each node which maintains a table that stores the DTQ values of the nodes in the same group or in the communication path. If the DTQ value for one node is lower than a threshold, this node is considered suspicious, and a voting procedure is triggered for the nodes in the group to collectively determine whether the node is compromised or not. In [11] for detecting the intruder in a sinkhole attack, authors first find a list of suspected nodes, and then identify the intruder from the list through a network flow graph effectively. Also robust to deal with cooperative malicious nodes that attempt to hide the real intruder, both numerical analysis and simulations, which confirm the effectiveness and accuracy of the algorithm, have been done.

III. The Proposed Algorithm

In this section we describe the proposed algorithm in details. For this purpose, the system model and energy consumption is first described, and then the proposed algorithm is explained.

A. Model of System and Consumption Energy

We use the same energy model as LEACH (Low Energy Adaptive Clustering Hierarchy) [12] algorithm. Let's d represents the distance between transmitter and receiver. Whenever d is greater than d_0, the multi-path model is used and the path loss coefficient is set to 4, otherwise the open space model is applied. In this case the path loss coefficient is set to 2. The above discussion is presented by the following equation:

$$E_{Tx}(l,d) = E_{Tx-elec}(l) + E_{Tx-amp}(l,d) = \begin{cases} lE_{elec} + l\varepsilon_{fs}d^2 & d < d_0 \\ lE_{elec} + l\varepsilon_{mp}d^4 & d \geq d_0 \end{cases}$$

where E_{elec} is the needed energy to activate the electronic circuits. ε_{mp} and ε_{fs} represent the activation energy of multi-path and open space models, respectively.

The energy consumption in the receiver side to receive L bit of data is calculated using the following equation.

$$E_{Rx}(l) = E_{Rx-elec}(l) = lE_{elec} = p$$

B. Algorithm Description

In the proposed algorithm, all network's nodes are similar and distributed randomly in the network. We assume that all network nodes know their location. At the beginning, the BS broadcasts its location to all nodes. The proposed work is appropriated for event driven applications. Whenever a node detects an event, a control packet is sent to the BS using single hop communication. The control packet contains the following information: the unique number of the control packet (id), the transmitter node (Nid), data packet identifier (Pid) and the size of the data packet (Psize).

After direct transmission of this packet to the BS, the transmitter node, depending on its routing table, sends data packet to its next hop node. The data packet is routed hop by hop until it recieves to the BS. When data packet is reached to the BS, the following three situations might be occurred:

- Data arrive at BS properly: when data arrives at BS, it is compared to the control packet and the accuracy of the data is determined.
- Data arrive at BS while manipulated: it means that the adversary node has changed data en route and transferred them to BS. BS detects this manipulation through comparing the data packet with the original control packet.
- Data packet never arrives at BS: the adversary node drops the packet and does not allow it to reach BS. When BS receives the control packet, it waits for a moment to receive the original data packet. Otherwise, it detects the existence of an adversary node in the network.

In cases 2 and 3, the malicious node disrupts the network. After receiving these two situations in the network, it looks for the malicious nodes and tries to remove them from the network routine.

C. Malicious Node Detection

After comprehending the existence of a malicious node in network, BS checks data transmission path and keeps existing nodes in its memory. Once BS detects existence of errors in a packet repeatedly, it checks the path each time and

compares the nodes kept in memory with the new path, keeping similar nodes in memory and deleting the remaining data. Accordingly, BS detects the malicious node, notifying other nodes not to transmit data to malicious node anymore.

IV. Simulation Results

In this section, using MATLAB simulation software we compare the performance of the proposed algorithm with that of [11]. The simulation parameters are given in Tab.1. In each round, an event occurs in network and sensor nodes transmit data event to the BS.

TABLE I: Simulation Parameters

Parameter	Value
Network's Radius	100m
Number of Sensor	100
Initial Energy	0.1 J
Eelec	50 nJ/bit
εfs	10 pJ/bit/m2
εmp	0.0013 pJ/bit/m4
Data Packet Size	4000 bits
Control Packet Size	32 bits
d0	87 m
Sinkhole Node	4

We compare the performance of proposed algorithm and algorithm [11] with respect to the number of rounds and detection of Sinkhole nodes. As Fig. 1 shows, the proposed method detects all the Sinkhole nodes after about 8 rounds. The network reliability is one of the important parameters of sensor networks. These quality service parameters can be defined in terms of the network capacity in detecting the events during the network lifetime. The more a network manages to report events (or the less it loses the events) the higher is its reliability.

In Fig. 2 comparison between two methods in terms of the number of lost events is shown. Obviously, the fact that a graph is lower shows that fewer events are missed by the algorithm. As the figure indicates, it is evident that the proposed algorithm is more reliable than CSW [11] algorithm in terms of event detection.

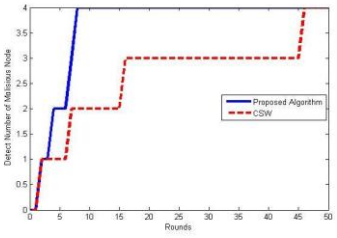

Fig. 1. Number of malicious nodes.

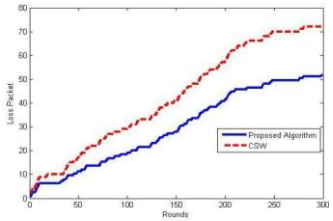

Fig. 2. Number of lost events.

V. Conclusion

In this paper, we present an algorithm for Sinkhole attack detection in wireless sensor networks. In the proposed method, the number of lost packets decreases and the detection of malicious and adversary nodes to be removed from the network occurs more expeditiously. As the number of lost events is decreased, the energy consumption is decreased too. Furthermore, the proposed algorithm can be used for detection of Wormhole attacks as well.

References

[1] F. Akyildiz *et al.*, "Wireless sensor networks: a survey," Computer Networks, March 2002.
[2] M. Saraogi, "Security in wireless sensor networks," *Communications of the ACM*, vol. 47, pp.53-57 , June 2004
[3] C. Karlof, N. Sastry, and D. Wagner, "TinySec: A Link Layer Security Architecture for Wireless Sensor Networks," *ACM enSys* 2004.
[4] A. Perrig, R. Szewczyk, V. Wen, D. Culler, and J. D. Tygar, SPINS: Security Protocols for Sensor Networks, MobiCom 2001.
[5] C. Karlof and D.Wagner, "Secure Routing in Sensor Networks: Attacks and Countermeasures," *First IEEE International Workshop on Sensor Network Protocols and Applications*, May, 2003.
[6] Al-S. K. Pathan, H.-W. Lee, and C. S. Hong, "Security in Wireless Sensor Networks: Issues and Challenges," in *Proceedings of 8th IEEE ICACT 2006*, vol. II, February 20-22, Phoenix Park, Korea, 2006, pp. 1043-1048
[7] C. K. D. Wagner, "In Secure Routing in Wireless Sensor Networks," Attacks and Countermeasures.
[8] W. R. P. Junior, *et al.*, "Malicious Node Detection in Wireless Sensor Networks," in *Proc. of the 18th International Parallel and Distributed Processing Symposium*, Apr 2004.
[9] Onat and I. A. Miri, "An Intrusion Detection System for Wireless Sensor Networks," in *Proc. of IEEE International conference on Wireless and Mobile Computing*, Networking and Communications, pp. 253-259, Aug 2005.
[10] T. Li, M. Song, and M. Alam, "Compromised Sensor Nodes Detection: A Quantitative Approach," in *Proc. of the 1st International Workshop on Wireless Security and Privacy*, pp.352-357, 2008.
[11] E. C. H. Ngai, J. Liu, and M. R. Lyu, "On the Intruder Detection for Sinkhole Attack in Wireless Sensor Networks," in *Proc. of IEEE ICC*, pp. 3383-3389, 2006.
[12] S. Lindsey and C. S. Raghavendra, "PEGASIS: Power Efficient Gathering in Sensor Informati-on Systems," in *the Proceedings of the IEEE Aerospace Conference*, Big Sky, Montana, 2002.

Maliheh Bahekmat was born on July 1980 in Mashhad, Iran. She received the BS and MS degree in computer engineering from the computer department, Islamic Azad University of Mashhad, Mashhad, Iran, in 2003 and 2008, respectively. She is a PhD candidate in computer engineering at computer department, Ferdowsi University of Mashhad. Her research interests are in computer networks, such as: wireless sensor and Smart grid networks.

Mohammad Hossien Yaghmaee was born on July 1971 in Mashad, Iran. He received his B.S. degree in Communication Engineering from Sharif University of Technology, Tehran, Iran in 1993, and M.S. degree in communication engineering from Tehran Polytechnic (Amirkabir) University of Technology in 1995. He received his Ph.D degree in communication engineering from Tehran Polytechnic (Amirkabir) University of Technology in 2000. He is currently an IEEE senior member. He has been a computer network engineer with several networking projects in Iran Telecommunication Research Center (ITRC) since 1992. November 1998 to July1999, he was with Network Technology Group (NTG), CandC Media research labs., NEC corporation, Tokyo, Japan, as visiting research scholar. September 2007 to August 2008, he was with the Lane Department of Computer Science and Electrical Engineering, West Virginia University, Morgantown, USA as the visiting associate professor. He is author of 3 books all in Farsi language. He has published more than 60 international conference and journal papers. His research interests are in Wireless Sensor Networks (WSNs), traffic and congestion control, high speed networks

including ATM and MPLS, Quality of Services (QoS) and fuzzy logic control.

Ashraf Sadat Heydari Yazdi was born on June 1988 in Mashhad, Iran. She received the BS degree in computer engineering from the computer department, Ferdowsi University of Mashhad, Mashhad, Iran, in 2010. She is a MS student in computer engineering at computer department, Ferdowsi University of Mashhad. Her research interests are in computer networks, wireless sensor networks, security and semantic web.

Sanaz Sadeghi was born on June 1988 in Mashhad, Iran. She received the BS degree in computer engineering from the computer department, Ferdowsi University of Mashhad, Mashhad, Iran, in 2010. She is a MS student in computer engineering at computer department, Ferdowsi University of Mashhad. Her research interests are in computer networks, wireless sensor networks and security.