Using Network Traffic to Infer Compromised Neighbors in Wireless Sensor Nodes

Conference Paper · January 2017

Lakshmi Narasimhan Srinivasan
Johns Hopkins University

Prahlad Suresh
Johns Hopkins University

Garth Crosby
Southern Illinois University Carbondale

Lanier Watkins
Johns Hopkins University

Using Network Traffic to Infer Compromised Neighbors in Wireless Sensor Nodes

J. M. Chandramouli[1], Juan Ramos[1], Lakshmi Srinivasan[1], Prahlad Suresh[1], Prashanth Kannan[1], Garth Crosby[2], Lanier Watkins[1]

[1]Johns Hopkins University, Baltimore, USA [2]Southern Illinois University Carbondale, USA

***Abstract*—This work introduces a novel security framework for wireless sensor networks (WSN) based on dynamic duty cycle, which allows nodes to detect their compromised neighbors based on unanticipated fluctuations in network traffic send rate over time. Our framework was assessed by its ability to detect advanced WSN threats (e.g., active, passive, or both attacks). One of the benefits of this framework is that it reduces all threats to unanticipated power dissipation. In other words, the framework assumes any neighbor not conforming to predicted power levels has been communicating with an unauthorized node, and thus is compromised. This threat model is emulated by applying pseudo random but bound (large to small) power dissipations to arbitrary nodes. Simulation results demonstrated that this framework was effective in detecting and isolating compromised sensor nodes.**

Keywords—Wireless Sensor Networks; WSN APT; Wireless Nodes; Power Levels

I. Introduction

A typical wireless sensor network consists of a set of sensors which are intended to sense or measure a physical property and transmit it to a concerned gateway in an efficient manner [1]. A typical wireless sensor network has a low passive power, relatively small memory capacity, and low computational power. Therefore within this context any security mechanism layered on top of the sensor nodes's duties must not be burdensome. This work is an extension of our previous work [6] in which we developed a novel Power Efficient Path Selection routing algorithm that extends the network lifetime by balancing the trade-off between residual sensor node energy and shortest path. In this paper, we leverage this routing algorithm and layer a low-overhead security protocol on top of it.

Researchers have proposed several mechanisms to detect or prevent malicious activities in WSNs. Some of the commonly used techniques are: (1) use of auto regressive detectors to identify malicious activity [2], (2) employing trust management schemes to prevent malicious activity [3, 9, 10], and (3) employing weights to high confidence nodes in the WSN [4]. In comparison to our approach, most of these concepts involve significant additional overhead in ensuring the security of the WSNs.

The main contribution of our work is an intrusion detection system (IDS) for WSNs that is: (1) low-power and low overhead and (2) applicable to multiple threat models (i.e., passive, active, and a combination of both).

$$E_{transmit/receive} = l*P_S(2E_{TX} + E_{fs}*d^2) \quad (1)$$

$$E_{transmit} = l*P_S(E_{TX} + E_{fs}*d^2) \quad (2)$$

II. WSN Threat Model

Wireless Sensor Networks are susceptible to a plethora of network-based attacks due to the broadcast-based communication used in these networks. These attacks can be both active and passive in nature. For traditional methods active attacks may be easier to detect, because there is normally network artifacts left behind. While passive attacks may be more difficult to detect because of the lack of network artifacts left behind. Both active (i.e., large power level reduction are experienced by the nodes that are attacked [5]) attacks and passive (i.e., small power level reductions are experienced by nodes used to launch attack) attacks reduce the power level of the victim node, and thus are detectable by our security framework.

We studied WSN attacks to better understand possible advanced threat models. The authors in [7] present a survey of active and passive attacks in WSNs.

III. WSN Security Model

As previously mentioned, we leverage the energy-aware dynamic duty cycling routing protocol proposed by Watkins et al. in [6]. Our security framework is implemented on top of this routing protocol.

A. Routing Layer

In [6], the wireless sensor nodes are based on the First Order Radio Model [8]. Dynamic duty cycling was added, which allows each node to modify its send rate to conserve its battery power level. The final wireless sensor network model dissipates energy per round based on equations 1 and 2 for transmitting and receiving, and Table 1 for dynamic duty cycling.

Table 1. Examples of duty cycle modes and send rates

Duty Cycle (%)	Effective Data Send Rate (kbps)	Energy Range
100	then $P_s = E_o(n)*10k$	if $E_{av}(n) >= 0.84* E_o(n)$
35.5	$P_s*0.355$	$E_{av} <0.84*E_o(n)$ and $>=0.68*E_o(n)$
11.5	$P_s*0.115$	$E_{av} <0.68*E_o(n)$ and $>=0.52* E_o(n)$

Where E_{TX} is the transmit and receive energy, E_{FS} is the free space energy, d is the distance between the nodes, P_s is the packet send rate, and l is the length of the packet used.

B. IDS Security Layer

Since each chosen path is based on the shortest path and made up with nodes with the most available battery power level, coupled with the fact that the network traffic send-rate and the battery power levels are correlated, there exists a unique opportunity for each node to infer the battery power level of its neighbor. We assume that the WSN is not compromised initially; instead, it becomes compromised sometime after the WSN is formed. If this assumption holds, neighbors should be able to identify compromised nodes based on the following steps: (1) from initial WSN setup, nodes observe the send-rate of their neighbors and infer their current power levels based on the logic from Table 1, coupled with calculating predicted power levels derived from the neighbor's initial power level (from setup) decremented by the theoretical dissipation due to the First Order Radio Model equations (See Equations 1 and 2), (2) nodes constantly compare their neighbors inferred power level to their predicted power levels, and (3) if the inference and predicted power levels are ever noticeably different, then a compromise is reported to the gateway. Next, the gateway must possess logic to determine when to remove the node from the network, but once the gateway makes this decision, encrypted messages must be sent to all nodes to omit the compromised node from the network.

IV. RESULTS AND DISCUSSION

The routing layer and IDS security layer were emulated using matlab. In the example run illustrated in Figure 1, node 42 attempts to establish a secure path between itself and the gateway node 34. The security framework establishes the most energy efficient and shortest path as the nodes identified in Table 2. In Table 2, node 7 determines that the predicted power level of node 22 is different from its inferred power level, and thus notifies the gateway. Assuming that the gateway's detection logic agrees that node 22 is compromised and it notifies the other nodes in the path of the compromise, Figure 2 illustrates the resulting behavior. The nodes in the path route around node 22, and thus Table 3 further illustrates the overall impact to the WSN, a secure path, but longer and a shorter lifetime.

V. CONCLUSION AND FUTURE WORK

In this paper, we propose an IDS framework for wireless sensor networks based on detecting discrepancies between inferred and predicted energy levels of neighboring nodes. Threat correlation is carried out using power loss measurement, and the compromised nodes are isolated by informing the gateway, which informs nodes to recalculate the path without using the isolated node. In future work, we would like to develop clear compromised node detection logic for the gateway. Currently, the gateway assumed any reported node is compromised.

Table 2. 50 node WSN, predicted vs. inferred power levels

Node	**42**	**22**	**7**	**6**	**34**
Predicted Power Level	0.021	0.029	0.055	0.021	0.094
Inferred Power Level	0.021	0.024	0.055	0.021	0.094

Table 3. Effects of node compromise on path attributes

	Original Path	**Revised Path**
Rounds	14	2
Length	126.24	128.26

VI. REFERENCES

[1] S. Rajasegarar, C. Leckie and M. Palaniswami, "Anomaly Detection in Wireless Sensor Networks," IEEE Wireless Communications, Vol. 15, No. 4, 2008, pp. 34-40.

[2] D. I. Curiac, O. Banias, F. Dragan, C. Volosencu and O.Dranga, "Malicious Node Detection in Wireless Sensor Networks Using an Autoregression Technique," 3rd International Conference on Networking and Services, Athens, 19-25 June 2007, p. 83.

[3] M. Momani and S. Challa, "Survey of Trust Models in Different Network Domain," International Journal Ad Hoc, Sensor & Ubiquitous Computing, 2010. doi:10.1109/MWC.2008.4599219

[4] L. Ju, H. Li, Y. Liu, W. Xue, K. Li and Z. Chi, "An Improved Intrusion Detection Scheme Based on Weighted Trust Evaluation for Wireless Sensor Networks," Proceedings of the 5th International Conference on Ubiquitous Information Technology and Applications, December 2010.

[5] A. Forootaninia, M. B. Ghaznavi-Ghoushchi, "An Improved Watchdog Technique based on Power-Aware Hierarchical Design for IDS In Wireless Sensor Networks", International Journal of Network Security & Its Applications (IJNSA), 2012.

[6] L. Watkins, G.V. Crosby, A. Sharmin, "Using network traffic to infer power levels in wireless sensor nodes," in *Computing, Networking and Communications (ICNC), 2014 International Conference on* , vol., no., pp.864-870, 3-6 Feb. 2014

[7] G. Padmavathi, D. Shanmugapriya, "A Survey of Attacks, Security Mechanisms and Challenges in Wireless Sensor Networks," International Journal of Computer Science and Information Security, IJCSIS, Vol. 4, No. 1 & 2, August 2009.

[8] W. R. Heinzelman, A. Chandrakasan, and H. Balakrishnan, "Energyefficient communication protocol for wireless microsensor networks," in the proceedings of the 33rd Hawaii International Conference on system sciences-HICSS, 2000.

[9] G. V. Crosby and Niki Pissinou, "Cluster based Reputation and Trust for Wireless Sensor Networks", in the proceedings of the IEEE Consumer Communications and Networking Conference, Jan. 2007.

[10] G.V. Crosby, Niki Pissinou and James Gadze, "A Framework for Trust-based Cluster Head Election in Wireless Sensor Networks", in the proceedings of the Second IEEE Workshop on Dependability and Security in Sensor Networks and Systems, April 2006

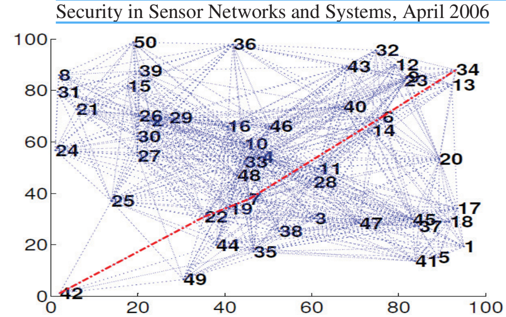

Figure 1. 50 node WSN, threat identified at node 22

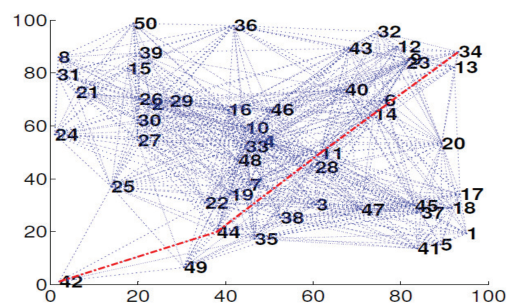

Figure 2. 50 node WSN, node 22 isolated