Sensor Intelligence for Tackling Energy-Drain Attacks on Wireless Sensor Networks

Udoh, E., Getov, Vladimir and Bolotov, A.

This is an electronic version of a paper presented at *the 23rd Workshop on Automated Reasoning: Bridging the Gap between Theory and Practice,* University of Liverpool, 19 to 20 May 2016.

SENSOR INTELLIGENCE FOR TACKLING ENERGY-DRAIN ATTACKS ON WIRELESS SENSOR NETWORKS

Ekereuke Udoh, Vladimir Getov, Alexander Bolotov
Distributed and Intelligent Systems Research Group
University of Westminster, 115 New Cavendish Street, London W1W 6UW
w1562173@my.westminster.ac.uk, V.S.Getov@westminster.ac.uk, A.Bolotov@westminster.ac.uk

Abstract. In this paper we propose a model for intelligent agents (sensors) on a Wireless Sensor Network to guard against energy-drain attacks in an energy-efficient and autonomous manner. This is intended to be achieved via an energy-harvested Wireless Sensor Network using a novel architecture to propagate knowledge to other sensors based on automated reasoning from an attacked sensor.

Introduction. Wireless Sensor Networks (WSN) form part of the architecture of the Internet of Things (IoT) and are known particularly for their resource-constrained nature due to the fact that these sensors are usually powered by batteries alongside their low processing power. This makes the WSN prone to energy-drain attacks, one of which is known as denial-of-sleep attack [1]. A number of approaches exists which aim to tackle these attacks; however these approaches rarely take into consideration the future scale of the IoT as predicted to expand exponentially in the coming years [2]. The implication of this is that approaches would need to be, not just energy-efficient but, autonomous in nature in order to withstand the variety of attacks that may arise as a result of a larger network where there is a wider attack surface.

Proposed Approach. The intended approach is an improvement of existing approaches - Gateway Media Access Control (GMAC) and Hierarchical Collaborative Model (HCM). While GMAC [3] and the hash-based scheme [4] use centralized approach via cluster heads, HCM [5] and the distributed wake-up scheme [6] use a distributed architecture. Although these approaches seem very useful, they do not take into consideration the size of the network especially on a large scale. Our proposed architecture is based on a combination of both the centralized and the distributed approach. It would involve the use of intelligent agents whereby each sensor becomes an agent which can sense data and take responsive action with the workload dynamically distributed among them. However, this would not function optimally with the current battery-powered sensors, but rather an energy harvested IEEE 802.15.4 wireless sensor network [2]. This is necessary because the dynamic distribution would lead to an increase in processing power thereby consequently increasing energy costs. In [7], the concept of virtual clusters is introduced whereby nodes are grouped into the same subnet and presented as a single resource. The WSN will be dynamically divided into clusters with cluster heads appointed for each cluster. In this approach, if a sensor encounters or senses an attack, it immediately takes responsive action and also broadcasts the information to the rest of the appointed cluster heads via a "rumour" approach which may consume more bandwidth than processing power. The "rumour" approach is coined from the term "routing by rumour", which explains the semantics of distance-vector routing protocols whereby each router sends messages to its nearest neighbour until the information propagates to all the routers. In this case, the cluster heads send information to the nearest cluster head and it continues that way until the information gets to all the cluster heads which then pass the information to their clusters. The cluster heads then relay this information to the sensors in their clusters.

High Level Constituents of the Approach

- Automated reasoning via intelligent agents
  In [8] a management scheme based on automated reasoning whereby Bayesian reasoning is used during the learning phase, is proposed to help protect against intrusions and also enhance energy-efficiency on a wireless sensor network. Threshold analysis is also used prior to the reasoning. In [9], the BayesMob algorithm is used for self-healing in a case where one or more sensor nodes fail. In this paper, we consider the Bayesian equation for predictive reasoning by sensors as a way of anticipating an attack and preventing it beforehand. More specifically, our model is based on the following Bayesian equation:

  $$P(A|B) = \frac{P(B|A)\,P(A)}{P(B)},$$

  where A and B are events
  - P (A) and P (B) are the probabilities of A and B without regard to each other.
  - P (A | B), a conditional probability, is the probability of observing event A given that B is true.
  - P (B | A) is the probability of observing event B given that A is true.

  In this context, for example, P (A) is the base rate or prior probability that a sensor is under attack. This could be based on a threshold value of the amount of energy being consumed by the sensor. P (B) could be the probability that the messages sent by the attacker have a certain size/frequency range. P (B|A) would then be the probability that a sensor under attack is receiving a certain message size/frequency range.

- Choice of WSN architecture
  A combination of centralized and distributed architecture is proposed. The centralized approach involves the use of clusters which are formed dynamically based on the location and proximity of sensors. Each cluster

has a cluster head which not only serves the other sensors but also acts as a proxy thereby hiding the identity of the sensors. At the cluster level, a single-hop architecture is used while a multi-hop architecture is used for communication between cluster heads. Because of its centralized approach, the single-hop architecture has low delay and a high channel capacity, while the multi-hop architecture which is distributed in nature has a high energy-efficiency and high signal-to-noise ratio [12].

- Resource availability (via energy-harvesting rather than battery-powered sensors)
  In [10], a relationship between autonomy and energy-efficiency is established whereby existing wireless sensor networks are limited by their battery power and therefore cannot be autonomous except more power is made available to them. Hence, energy-harvesting is proposed. In [11], the need for energy harvesting is also acknowledged considering that the existing battery-powered sensor nodes need periodic maintenance which contradicts with the characteristics of autonomous systems.

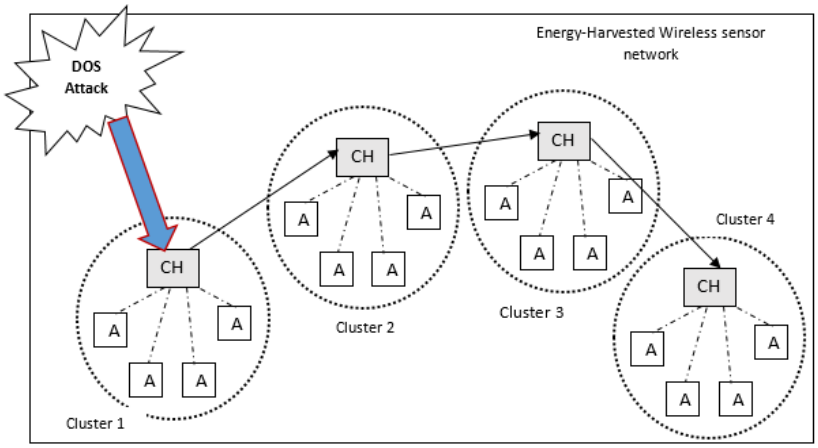

Figure 1: Proposed Wireless Sensor Network Architecture for Intelligent Agents (Sensors)

Figure 1 above shows an attack being directed at a cluster head. The cluster head (CH) is an intelligent agent and also acts as a proxy for the member-nodes of its cluster. The moment it realizes it is under attack, it appoints one of its members as a cluster head and isolates itself from the network thereby allowing communication to continue. The learned information is then passed to other cluster heads to enable them to easily prevent the attack, in case they become the new target.

Conclusions. Our novel architecture is intended to fit into the big picture of providing an energy-efficient and autonomous security on the IoT. Currently, the proposed approach is being tested on a simulator and the results will be analysed and discussed in the context of energy-efficiency and other existing approaches.

REFERENCES

[1] A. Merlo, M. Migliardi, and L. Caviglione, "A survey on energy-aware security mechanisms," *Pervasive Mob. Comput.*, vol. 24, pp. 77–90, 2015.

[2] B. Tourancheau, F. Rousseau, A. Duda, L. Damon, and R. Guizzetti, "Energy Cost of Security in an Energy-Harvested IEEE 802.15.4 Wireless Sensor Network," pp. 198–201, 2014.

[3] M. I. Brownfield, M. I. Brownfield, and N. J. Davis, "Energy-efficient Wireless Sensor Network MAC Protocol Energy-efficient Wireless Sensor Network MAC Protocol," *Management*, 2006.

[4] M. Pirretti, S. Zhu, N. Vijaykrishnan, P. Mcdaniel, M. Kandemir, and R. Brooks, "The Sleep Deprivation Attack in Sensor Networks: Analysis and Methods of Defense," *Int. J. Distrib. Sens. Networks Int. J. Distrib. Sens. Networks Int. J. Distrib. Sens. Networks*, vol. 2, no. 03, pp. 267–287, 2006.

[5] T. Bhattasali, "Sleep Deprivation Attack Detection in Wireless Sensor Network," *Int. J. Comput. Appl.*, vol. 40, no. 15, pp. 19–25, 2012.

[6] F. J. Wu and Y. C. Tseng, "Distributed wake-up scheduling for data collection in tree-based wireless sensor networks," *IEEE Commun. Lett.*, vol. 13, no. 11, pp. 850–852, 2009.

[7] S. Isaiadis and V. Getov, "Integrating Mobile Devices into the Grid: Design Considerations and Evaluation," *Proc. of Euro-Par 2005 Conference, LNCS*, vol. 3648, pp. 1080-1088, Springer, 2005.

[8] H. Khalife and F. Krief, "Reasoning Services for Security and Energy Management in Wireless Sensor Networks," *Proc. 7th Int. Conf. Netw. Serv. Manag.*, pp. 520–524, 2011.

[9] M. Coles, D. Azzi, and B. Haynes, "A self-healing mobile wireless sensor network using predictive reasoning," *Sens. Rev.*, vol. 28, no. 4, pp. 326–333, 2008.

[10] R. Vullers, R. Schaijk, H. Visser, J. Penders, and C. Hoof, "Energy harvesting for autonomous wireless sensor networks," *IEEE Solid-State Circuits Mag.*, vol. 2, no. 2, pp. 29–38, 2010.

[11] A. Lambebo and S. Haghani, "A Wireless Sensor Network for Environmental Monitoring of Greenhouse Gases," p. 2010, 2014.

[12] A. K. Singh, S. Rajoriya, S. Nikhil, and T. K. Jain, "Design constraint in single-hop and multi-hop wireless sensor network using different network model architecture," *Int. Conf. Comput. Commun. Autom.*, pp. 436–441, 2015.