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

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 4, April 2016

A Review on Optimization of an Improved Watchdog Mechanism in Wireless Sensor Networks

Vinod.R[1] and Dr.D.Jayaramaiah[2]

M.Tech Student, Dept. of ISE, The Oxford College of Engineering, Bangalore, India[1]

Professor and Head, Dept. of ISE, The Oxford College of Engineering, Bangalore, India[2]

ABSTRACT: Wireless Sensor network (WSN) are broadly used today in various fields such as environmental control, surveillance task, object tracking, military applications etc. Watchdog is a monitoring technique which detects the misbehaving nodes in the network. Watchdog technique is a fundamental building block to many trust systems that are designed for securing wireless sensor networks (WSNs). Optimizing the watchdog techniques can save energy without sacrificing much and also enhance the protection against certain attacks. The main focus of this paper is to focus on how an improved watchdog technique can be used for optimization to improve the results.

KEYWORDS: Watchdog, Wireless sensor network, Optimization, Energy saving, topology approaches

I. INTRODUCTION

A wireless sensor network is an ad-hoc network which consists of large number of small inexpensive devices which are known as nodes (motes)[1][2]. These nodes are battery operated devices capable of communicating with each other without relying on any fixed infrastructure. The wireless sensor networks (WSNs) are often deployed in such an environment which is physically insecure and we can hardly prevent attackers from the physical access to these devices.WSN consists of base station along with number of nodes that sense the environment and send data to the base station. The base station (sink) is more powerful than other nodes in terms of energy consumption and other parameters and serves as an interface to the outer world. When any node needs to send a message to the base station that is outside of its radio range, it sends it through internal nodes. The internal nodes deployed in WSNs are the same as others, but besides of local sensing they also provide forwarding service for other nodes.

A Wireless Sensor Network (WSN) is a specialized wireless network that is composed of a number of sensor nodes deployed in a specified area for monitoring environment conditions such as temperature, air pressure, humidity, light, motion or vibration, and can communicate with each other using a wireless radio device[3]. WSNs are powerful in that they are amenable to support a lot of very different real-world applications; they are also a challenging research and engineering problem because of this very flexibility. Most sensor network protocols assume a high degree of trust between nodes in order to eliminate the overhead of authentication. This creates the risk of attackers introducing malicious nodes to the network, or manipulating the operation of existing nodes. Consequently, there is the potential for a wide variety of attacks on sensor networks. An intrusion is defined as a set of actions that compromises confidentiality, availability and integrity of a system. Intrusion detection is a security technology that attempts to identify those who are trying to break into and misuse a system without authorization and those who have legitimate access to the system but are abusing their privileges. The system can be a host computer, network equipment, a firewall, a router, a corporate network, or any information system being monitored by an intrusion detection system.

The rest of the paper is organized as follows: Section II discusses about the first watchdog mechanism introduced. In Section III discusses about the Improved Watchdog mechanism and its improvements. Section IV discusses the review of optimizing of an improved watchdog mechanism. In Section V concludes the paper based on the literature review.

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

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 4, April 2016

II. WATCHDOG MECHANISM

In [1], [4] and [5], the watchdog mechanism is one of the intrusion detection techniques in Wireless Sensor Network. Watchdog is a monitoring technique which detects the misbehaving nodes in the network. As shown in Fig. 1 consider a node A which wants to send a message to node C which is not in its radio range.

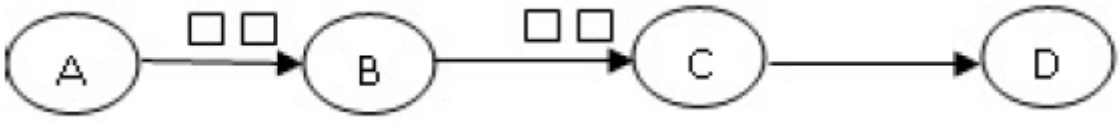

Fig. 1. Packet transmission between nodes

As a result of which it sends the message through an intermediate node B. When the node B receives a packet from A it then forwards it to C. Here we may consider SA be a set of nodes which hear messages sent from A to B and SB be a set of nodes that hear message from B to C. In this way we may define a set of possible watchdogs of the node B as an intersection of SA and SB. This means that any node that lies in the intersection region is able to hear both messages and is able to decide whether node B forwards message from node A. This approach relies on the broadcast nature of wireless communications and the assumption that sensors are usually densely deployed[1]. When a message is broadcasted in a network the packet is not only received by the intended node but it is also received by the neighboring nodes within that range. Normally such nodes should discard the packet, but this can be used for intrusion detection. Hence, a node can activate the IDS agent and monitor the packets that are sent by its neighbors by overhearing them.

III. IMPROVED WATCHDOG MECHANISM

A. *Mechanism:*

In [6], a new technique based on Watchdog mechanism which is modified and improved by enhancing the security in wireless sensor network. We call this technique I-Watchdog (Improved Watchdog). Unlike the basic technique in which the node A is assumed to be the watchdog, in I-Watchdog technique, as shown in Figure 2, the cluster heads (nodes that are responsible for monitoring each cell) are assumed to be as the first layer watchdogs.

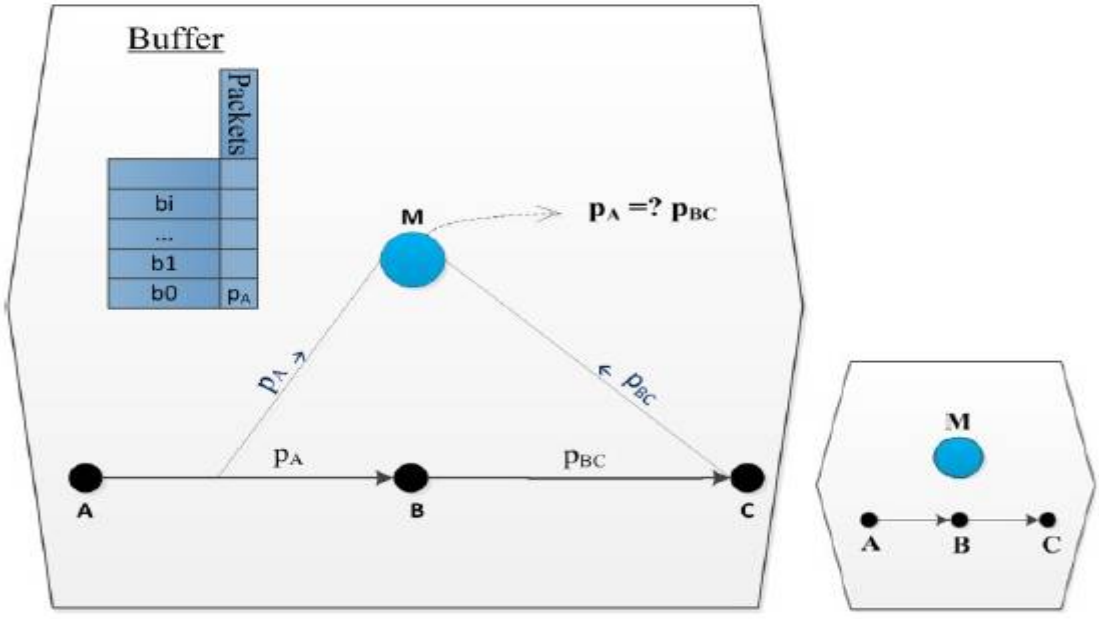

Fig. 2. Improved-Watchdog (I-Watchdog)

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

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 4, April 2016

In this approach, if a node for example A wants to send a message to a node say C, the cluster head node (M) operates as watchdog. As shown in Fig. 2, the cluster head node uses a buffer which accommodates all the sent items by the nodes within its sensory limit. Since the node B is an interface between A and C, it eavesdrops the first sending of the node B after receiving the message from A and compares it with the message in the buffer. If the messages are similar, the first message in the buffer will be deleted. Otherwise, it will turn out that the node B has not sent the message or replaced it with another one. We assume that the buffer used by Watchdog in this technique, as the Fig. 2 show, has been divided into cells like b_0, b_1, b_2, …, b_i, …and bn. According to malicious node detection algorithm which will be discussed below, and using the below equation value, we can determine whether or not the message sent from A to B will be correctly sent to C (the target node).

Here, P_{BC} refers to the packet to be sent to C by B.

$$F_i = b_i - P_{BC} \qquad \forall 0 \leq i \leq n \tag{1}$$

B. *Description of the Algorithm:*

The steps of the algorithm for malicious node detection are as follow:

1. A sends a packet to C via B. Meanwhile, M (the cluster head node) eavesdrops the packet and saves a copy in its counterpart section in buffer b.
2. The node M eavesdrops to the communication between B and C for t second (this time depends on the nodes processing and sending speed as well as the sensors type) and refers to the step 5 in the case of not receiving any packet.
3. The F_i value is calculated if M eavesdrops to the packet PBC.
4. If F_i=0, the message in cell *bi* (where its counterpart message has been saved in buffer b) will be deleted and the algorithm moves to the step 6. If $F_i \neq 0$, the message remains in the buffer and moves to step 5.
5. The warning message, signaling the maliciousness of the node B, is sent to the upper layer by the cluster head node.
6. The end of algorithm.

As mentioned above, in the case of entering the step 5, the cluster head node sends a warning message to the upper layer. If the warnings reach a specific limit, the cluster head node introduces B as a malicious node.

IV. OPTIMIZATION OF THE WATCHDOG MECHANISM

In [7], Peng Zhou, Siwei Jiang, Athirai Irissappane, Jie Zhang, Jianying Zhou, and Joseph Chee Ming Teo have proposed watchdog optimization techniques whose optimization goal is to minimize the energy cost of the whole WSN and to maximize security (in terms of trust accuracy and trust robustness). They have proposed optimization on the first watchdog approach. There are two techniques for watchdog optimization: one is watchdog location optimization and the other is watchdog frequency optimization. In watchdog location optimization, the optimal watchdog positions are identified. Once the optimal node is identified where on which the watchdog mechanism has to be performed, the selection of nearby neighbor node of that optimal node will perform the watchdog mechanism in order to reduce its energy cost. The algorithm proposed here is DBP (Distance Based Probabilistic) algorithm. In the DBP algorithm, the watchdog node selection probability should be larger in case the neighbor node is close to the target node. DBP algorithm can resist discrimination attack due to the probabilistic selection manner and the maintenance of some watchdog node redundancy. In watchdog frequency optimization, based on the watchdog mechanism frequency of use certain trust-system mechanisms are used in order to overcome the limitations of the watchdog mechanism. When watchdog nodes have been determined, the next optimization point is to find the minimal number of required watchdog tasks to save energy but keep security in a sufficient level. The algorithm they proposed here is HWFA (heuristic watchdog frequency adjustment) algorithm. In the HWFA algorithm, watchdog frequency is adjusted adoptively by referencing trust worthiness. In the HWFA algorithm, there are two design goals: one is that the watchdog frequency should increase when the trust worthiness grows up from 0 to 0.5 but decrease when it climbs from 0.5 to 1, and the other is that the smallest should not be 0. The first design goal is to ensure that the watchdog frequency is high if the target node is uncertain but low if the target is determined. The second design goal is to guarantee that the watchdog

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

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 4, April 2016

node never disables the monitoring to the target node at any time. All these techniques are applied on flat topology approach.

In [6], A. Forootaninia and M. B. Ghaznavi-Ghoushchi have proposed an improved watchdog technique on hierarchical approach. In their hierarchical approach, their watchdog mechanism is performed only on the cluster-head nodes. There are different levels of cluster-head nodes which monitors their lower level nodes. In the hierarchical approach, the cluster-head nodes and its higher level nodes remain static whereas the lowest level sensor nodes can be dynamic. The optimization approach mentioned above can be used in such hierarchical approach where the optimization techniques like the watchdog location optimization might give a better result. In this case, since the watchdog mechanism is applied only on the cluster-head nodes, identifying the optimal node that performs watchdog mechanism can be easily identified. The improved watchdog mechanism has overcome most of the limitations of its previous watchdog approach, the watchdog frequency optimization can be used for referencing the trust worthiness to overcome the remaining limitations of the improved watchdog approach.

V. CONCLUSION AND FUTURE WORK

The watchdog optimization techniques that was proposed on watchdog mechanism of a flat topology approach has been successfully resulted that it can save at least 39.44% of energy without sacrificing much security and enhance the protection against certain attacks. Suppose if these optimization techniques are used on the improved watchdog mechanism of a hierarchical approach, it has possibility of saving more energy.

In future, we can make use of Peng Zhou, Siwei Jiang, Athirai Irissappane, Jie Zhang, Jianying Zhou, and Joseph Chee Ming Teo optimization techniques on A. Forootaninia and M. B. Ghaznavi-Ghoushchi improved watchdog approach where it can overcome certain challenges like dynamic approach, load balancing, etc.

REFERENCES

1. Jijeesh Baburajan, Jignesh Prajapati, “A Review Paper on Watchdog Mechanism in Wireless Sensor Network to eliminate False Malicious node Detection”, International Journal of Research in Engineering and Technology (IJRET), Vol.3, Issue 1, pp.381-384, Jan 2014.
2. Bc. Lumír Honus, “Design, implementation and simulation of intrusion detection system for wireless sensor networks”, Brno, spring 2009.
3. A. Babu Karuppiah and S. Rajaram, “False Misbehavior Elimination of Packet Dropping Attackers during Military Surveillance using WSN”, Advances in Military Technology (AiMT), Vol. 9, No. 1 pp. 19-30, June 2014.
4. Sergio Marti, T. J. Giuli, Kevin Lai, “Energy Mitigating routing misbehavior in mobile adhoc networks”, in MobiCom ’00: Proceedings of the 6th annual international conference on Mobile computing and networking, pp.255–265, New York, NY, USA, 2000.
5. Abror Abduvaliyev, Al-Sakib Khan Pathan, “On the Vital Areas of Intrusion Detection Systems in Wireless Sensor Networks”, in IEEE Communications Surveys & Tutorials, Vol. 15, Issue 3, Third Quarter 2013.
6. A. Forootaninia and 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), Vol.4, Issue 4, pp.161-178, July 2012.
7. Peng Zhou, Siwei Jiang, Athirai Irissappane, Jie Zhang, Jianying Zhou, and Joseph Chee Ming Teo, “Toward Energy-Efficient Trust System Through Watchdog Optimization for WSNs”, IEEE transactions on Information forensics and security, Vol. 10, Issue 3, pp.613-625, March 2015.

BIOGRAPHY

Vinod.R a Student of Information Science and Engineering Department at The Oxford College of Engineering-Bangalore, affiliated to VTU pursuing M.Tech in Computer Networking and Engineering. He received his Bachelors of Engineering in Computer science and Engineering from New Horizon College of Engineering-Bangalore affiliated to VTU. His research interests are Computer Networks (wireless sensor networks, Internet of Things (IOT) and LTE).

Dr.D.Jayaramaiah an Alumni of IIT-Delhi with thirty five years of experience in Telecom, Software, IT industry and R&D at Defence Labs has been actively involved with state of art technology development application software development. Earlier he was head R&D of L&T InfoTech, Bangalore Division. Currently he is heading Information Science and Engineering Department at The Oxford College of Engineering-Bangalore, affiliated to VTU. His research interests are Next Generation Mobile Networks, Mobile Agent Technology and Network Management Systems. He is a Fellow of the IETE and Senior Member CSI and senior member PMI-USA. He has presented Seventeen Research Papers at various International Conferences organized by IEEE, World Wireless Congress, 3GMF, 4GMF and IASTED.