Hindawi Publishing Corporation
International Journal of Distributed Sensor Networks
Volume 2015, Article ID 848636, 9 pages
http://dx.doi.org/10.1155/2015/848636

Research Article

An Intrusion Tolerance Method Based on Energy Attack for Wireless Sensor Network

Yu Jiang and Jie Huang

Information Science and Engineering School, Southeast University, Nanjing 210096, China

Correspondence should be addressed to Yu Jiang; jiangyu@seu.edu.cn

Received 2 December 2014; Revised 23 March 2015; Accepted 24 March 2015

Academic Editor: Roland Rieke

Wireless sensor network is vulnerable to malicious attacks because of the broadcast nature of wireless signal. In order to overcome the shortcomings of existing methods, this paper presents an intrusion tolerance method against malicious nodes. Different from the traditional intrusion tolerance methods based on encryption, authentication, and multirouting, the proposed method uses active protection to achieve intrusion tolerance. Small power consumption of many normal nodes is exchanged for large power consumption of relatively small number of malicious nodes to decrease the lifetime of malicious nodes. Theoretical analysis and test results show that the proposed methods not only prolong the lifetime of the sensor network but also achieve the effective protection against malicious nodes. The active protection method provides new ideas for the security in WSN.

1. Introduction

Wireless sensor network (WSN) is currently being considered for many applications, including industrial application, security surveillance, medical equipment, environment, and weather monitoring. It is rapidly growing due to its importance and relevance to both research community and commercial applications. Small, low-cost, low-power, and multifunctional sensor nodes become possible due to technology development [1]. WSN is composed of communication nodes with sensing, computation, and wireless communication capabilities. These nodes are typically resource-constrained with limited energy and hardware [2]. All the nodes are working together to collect different types of data and communicate with each other. WSN has been increasingly deployed for applications in harsh and inaccessible places, so each individual sensor node can be easily captured, destroyed, and compromised by malicious attacks due to lack of security.

Various WSN intrusion issues have recently brought significant economic losses which exacerbated people's concerns on its security. Therefore, intrusion tolerance started to be widely studied in recent years. As an active security mechanism, intrusion tolerance technology can extend a network's lifetime. Intrusion tolerance system (ITS) [3] is the third-generation network security technology, which is different to the first and second generation. The first generation of network security technology takes defense as the main means while the second generation has the main means to detect intrusions. The technology of network intrusion tolerant accepts the presence of weak points and assumes that these vulnerabilities can be exploited by intruders. It does not concern how to defend or detect intrusions but considers how to shield or contain intrusions effectively and continues to ensure the system with data confidentiality, integrity, and external services availability. The above functions of ITS were originally proposed for the Internet [4] which makes existing security mechanisms of ITS not suitable for the WSN. It is imperative to design intrusion tolerance into WSN so that the overall sensor network functionalities can be sustained without interruption by malicious attacks.

In this paper, an intrusion tolerance method based on the energy attack (ITMEA) is proposed to defend malicious attacks. ITMEA is mainly designed to realize intrusion tolerance rather than intrusion detection though it can be integrated with intrusion detection method. There are three notable features of ITMEA that make it a new and efficient solution for WSN, as listed in the following.

(1) Normal nodes use energy attacks during their sleep period to deal with the malicious nodes to decrease their lifetime.

(2) ITMEA is implemented whether the malicious nodes exist or not.

(3) ITMEA shows different performance to different attacks.

The remainder of this paper is organized as follows. In Section 2, state-of-the-art intrusion tolerance techniques for WSN are discussed. Section 3 proposes ITMEA method and theoretical analysis. Simulation results and test analysis are presented in Section 4. Finally, the conclusion is addressed in Section 5.

2. Intrusion Tolerance Techniques in WSN

Intrusion tolerance is the capability to keep systems working correctly during occurrence of malicious attacks. Due to the unique features of WSN, combinations of threats, which are not normally faced by traditional wired and wireless networks, have to be considered. These threats are vulnerable to a variety of security attacks. A great deal of work has been done to address the sensor network security problems recently which make WSN be able to tolerate intrusions.

The security protocol is the first kind of intrusion tolerance techniques to provide confidentiality, freshness, and authentication. Perrig et al. [5] proposed Security Protocols for Sensor Networks (SPINS), which is a suite of security protocols optimized for WSN. SPINS has two secure building blocks: Secure Network Encryption Protocol (SNEP) and the "micro" version of Timed Efficient Stream Loss-Tolerant Authentication (μTESLA). SNEP includes data confidentiality, two-party data authentication, and evidence of data freshness. μTESLA provides authenticated broadcast for severely resource-constrained environments. Zhu et al. [6] proposed Localized Encryption and Authentication Protocol (LEAP), which is a key management protocol for sensor networks. LEAP supports establishment of four types of keys for each sensor node and also includes an efficient protocol for internode traffic authentication based on the use of one-way key chains. Park and Shin [7] presented Lightweight Security Protocol (LiSP) to offer efficient key broadcast, authentication for each key-disclosure, the ability to detect/recover lost keys, seamless key refreshment, and robustness to internode clock skews. TinySec [8] is the first fully implemented link layer encryption mechanism for WSN and addresses the extreme resource constraints of sensor nodes with careful design. It has been incorporated into the official TinyOS release. MiniSec [9] and TinyECC [10] are also designed to run under TinyOS to implement secure communication. ContikiSec [11] and FlexiSec [12] focus on secure network protocol of WSN. ContikiSec, which is designed for the Contiki Operating System, has a configurable solution with confidentiality, authentication, and integrity. FlexiSec provides a configurable link layer security architecture wherein an application can be compiled flexibly, with respect to its actual security demands. A link layer security protocol called WSNSec [13] combines the advantageous aspects of the Scalable Encryption Algorithm (SEA) with the Counter Mode (CTR) and Cipher Block Chaining-Message Authentication Code (CBC-MAC) approaches to provide data confidentiality, message authentication, and integrity functions. In the secure network protocol of MoteSec-Aware [14], a Virtual Counter Manager (VCM) with a synchronized incremental counter is presented to detect the replay and jamming attacks based on the symmetric key cryptography using Advanced Encryption Standard (AES) in Offset Codebook (OCB) mode.

Redundancy management is the second kind of intrusion tolerance techniques. Deng et al. [15, 16] introduced redundant multipath routing to improve intrusion tolerance by bypassing malicious nodes. The main idea of their approaches is to use multipath and/or multiple base stations combined with cryptography mechanisms to improve the intrusion-tolerant capability of WSN. Al-Hamadi and Chen [17] propose redundancy management of Heterogeneous Wireless Sensor Networks (HWSNs), utilizing multipath routing to answer user queries in the presence of unreliable and malicious nodes. Hemalatha and Venkatesh [18] analyze redundancy management for multipath routing to find a reliable path and detect unreliable nodes by discarding the path. The redundant node scheme of Wei and Kim [19] can prolong the lifetime of network and isolate malicious traffic introduced through compromised nodes or illegal intrusions.

Trust model is the third kind of intrusion tolerance techniques. The reputation-based framework for sensor network (RFSN) [20] is the first trust model designed and developed for sensor networks. It makes use of watchdog mechanism to build reputation and trust rating of node. Extended watchdog [21] mechanism is used to monitor all its neighbors' behavior based on direct observations of information collected from MAC layer. The Retrust [22] is an attack-resistant and lightweight trust management scheme to detect faulty or malicious behaviors with a two-tier architecture and improve the security requirements of medical sensor network. A lightweight and dependable trust system (LDTS) [23] for clustered WSNs uses direct trust and feedback trust to improve decision making and collaborative processing by detecting malicious behaviors. The Sensor Trust [24] is a resilient model for improving data integrity. It evaluates the trust worthiness of node in hierarchical WSN using past history and recent risk to accurately identify the current trust level. A highly scalable cluster-based hierarchical trust management protocol [25] is proposed to derive multidimensional trust attributes from communication and social networks to evaluate the overall trust of a sensor node.

3. ITMEA

A WSN is an energy-constrained system which minimizes power consumption in order to extend the lifetime of WSN. Some malicious attacks target the power supply of a sensor node. One of such threats is called denial-of-sleep attack, a specific type of denial-of-service (DoS) attack [26] which tries to exhaust the node's battery power supply. The impacts of DoS attacks can significantly reduce the network lifetime from months or years to days. The attacker however has similar constraints as those of victims.

The malicious nodes in a number of wireless sensor network models are assumed to have unlimited energy and

Table 1: Wireless sensor chip current consumption.

	CC2430	CC2530
Power down mode	0.5 μA	1 μA
MCU active mode	5.1 mA with 16 MHz OSC	3.4 mA with 16 MHz OSC
RX mode	26.7 mA	24.3 mA
TX mode	26.9 mA (0 dBm output power)	33.5 mA (4.5 dBm output power)

resources which are not applicable for practical applications. Nowadays, large numbers of sensor nodes are densely deployed over a wide region for monitoring complicated environment. In some regions, replacement or recharging of the node is impossible. For malicious nodes, to analyze the situation in which the nodes' energy can be exhausted is more meaningful than that without energy constraints.

There are two widely used wireless sensor node chips, CC2430 and CC2530. Each chip has its own platform configured to run for more than one year by using a pair of AA batteries and wakeup/sleep protocol. The chips are working in four different modes: (1) power down mode with external interrupt or timer active; (2) MCU active mode with normal functions on; (3) MCU active and RX mode with RX on; (4) MCU active and TX mode with TX on. Table 1 shows the typical current consumption under different modes and Table 2 shows the working days of chips with four modes by two standard 3,000 mAh AA batteries.

Table 1 illustrates the importance of making a node asleep. It is because that, in the TX and RX mode, the power consumption can be up to five orders of magnitude greater than the power down mode. It is necessary to put the chip into power down mode to save the battery power when it is not sending or receiving data. As shown in Table 2, the disparity of the working days between radio on mode (TX and RX mode) and power down mode is significant. Therefore, increasing or decreasing the time of the radio on/power down mode can have dramatic impact on the network lifetime.

As it is mentioned above, the malicious nodes are power constrained in most situations. The lifetime can be minimized if the malicious nodes are always in the radio on mode. In some intrusion detection systems (IDS), malicious attacks can be detected and the attacking nodes will be located and destroyed. However, in regard to the huge number of sensor nodes and their hard working environment, the approach to destroy nodes is not feasible and worthy. Even though the malicious nodes are detected and located, the network has to execute mechanisms to defend attacks as long as the malicious nodes are in their lifetime, which will consume power of normal nodes. Therefore, the most efficient method to extend the network's lifetime is to make the malicious nodes exhaust their limited power as soon as possible instead of finding and destroying them. Different from the traditional intrusion tolerant method based on encryption, authentication, and multirouting, ITMEA is proposed to make the normal nodes attack the malicious nodes actively to exhaust their power. The comparison between traditional and proposed methods is carried out in Section 5 to prove the efficiency of our method.

Table 2: Working days of the wireless sensor chip.

	CC2430	CC2530
Power down mode	250000	125000
MCU active mode	24.5	36.7
RX mode	4.7	5.1
TX mode	4.6	3.7

3.1. Network Framework and Fault Model. The WSN considered in this paper consists of two kinds of static nodes: sensor node and sink node. The structure of WSN is not limited, for example, cluster-based and tree-based. It is assumed that the sink node which is provided with high computational capabilities, large storage, and unlimited energy cannot be compromised by malicious nodes and the sensor nodes have the same resources (energy, computation, and communication capabilities).

The assumptions of the capabilities of an adversary are listed as follows.

(1) An adversary can capture sensor nodes and is capable of compromising a sensor node to obtain all of its information. In addition, a sensor node can be reprogrammed to convert it into a malicious node to implement network-layer attacks.

(2) An adversary can receive any data from any sensor node or sink node within its receiving range and physically move from place to place.

(3) Malicious nodes can be heterogeneous with powerful computation and storage capabilities but are power-constrained as sensor node.

3.2. Characteristic of Different Network-Layer Attacks. Before discussion about the details of ITMEA, the characteristic of different network-layer attacks is analyzed to explain the feasibility of the method. In this paper, five types of malicious attacks are studied: (1) selective forwarding attack, (2) wormhole attack, (3) Sybil attack, (4) sinkhole attack, and (5) hello flood attack.

Selective forwarding attack is an ordinary attack. If a malicious node in the data forwarding path initiates a selective forwarding attack, malicious node refuses to forward sensitive messages or simply drops the messages ensuring that they are not propagated any further, resulting in the fact that the base station cannot receive integrated messages. When the adversary is in the forwarding path, the selective forwarding attack can be the most effective and hard to detect. When a malicious node hears a message M, its power consumption E_{c1} can be expressed as

$$E_{c1} = \frac{p\left(I_{\mathrm{TX}} + I_{\mathrm{MCU}}\right) L_M}{v} + \frac{\left(I_{\mathrm{RX}} + I_{\mathrm{MCU}}\right) L_M}{v}, \qquad (1)$$

where v is the bit rate of the node, L_M is the length of M in bits, I_{MCU} is the MCU current consumption with normal

CPU activity, I_{TX} is current consumption of radio in TX mode, and I_{RX} is current consumption of radio in RX mode. E_{c1} is a statistical value as p is the probability whether the malicious node forwards the message or not. Actually, E_{c1} indicates the least power consumption of hearing a message because the node always needs to spend more time than L_M/v to receive the entire message M.

In a wormhole attack, one malicious node receives a packet at one location in the network. Then, it tunnels the packet to another malicious node at another location and replays it. Wormhole tunnels can be occurring by means of a wired link, a high quality wireless out-of-band link, or a logical link via packet encapsulation. When a malicious node hears a message M, it has to retransmit the message and its power consumption E_{c2} can be expressed as

$$E_{c2} = \frac{(I_{\mathrm{TX}} + I_{\mathrm{MCU}})\, L_M}{v} + \frac{(I_{\mathrm{RX}} + I_{\mathrm{MCU}})\, L_M}{v}. \quad (2)$$

In a Sybil attack, malicious node has multiple identities. The malicious node can fabricate a new identity or steal an identity from a legitimate node. Therefore the malicious node can act as different nodes with different identities. When a malicious node hears a message M, it will repeat the message with different identities and its power consumption E_{c3} can be expressed as

$$E_{c3} = n\left[\frac{(I_{\mathrm{TX}} + I_{\mathrm{MCU}})\, L_M}{v} + \frac{(I_{\mathrm{RX}} + I_{\mathrm{MCU}})\, L_M}{v}\right], \quad (n \geq 2). \quad (3)$$

It is well-known that the many-to-one communication is highly vulnerable to the sinkhole attack. In a sinkhole attack, malicious node typically works by attracting surrounding nodes with unfaithful routing information and tricks other nodes into forwarding messages to them. A sinkhole attack prevents the sink node from obtaining data and threats higher-layer applications. When a sinkhole is established, the malicious node can then implement the selective forwarding attack and wormhole attack. The power consumption E_{c4} of the sinkhole attack on hearing a message is between E_{c1} and E_{c2} and E_{c1} can be taken as its expression.

In a hello flood attack, malicious node broadcasts large quantities of useless data packets to neighbor nodes in its communication range. It can simply rebroadcast overhead packets to be received by other nodes in the network. This attack can flood hello request to any legitimate node and break the security of WSN. When a malicious node hears a message M, it will repeat the message to all the nodes in the network where the node number is N and its power consumption E_{c5} can be expressed as

$$E_{c5} = N\left[\frac{(I_{\mathrm{TX}} + I_{\mathrm{MCU}})\, L_M}{v} + \frac{(I_{\mathrm{RX}} + I_{\mathrm{MCU}})\, L_M}{v}\right]. \quad (4)$$

3.3. The Details of ITMEA

3.3.1. The Time Frame of a Normal Node. ITMEA divides a time frame into normal working and intrusion tolerance periods and the normal working period is further divided into a synchronization period and a data transfer period which is shown in Figure 1. The time of normal working and intrusion tolerance period is T_1 and T_2, respectively. The synchronization period represented by T_s allows nodes to periodically announce their sleep schedules to correct network time drift and synchronize with the other nodes in the network. The synchronization protocol of SMAC [27] is embedded in the proposed method. The data transfer period represented by T_d maintains the normal working functions of WSN and the intrusion tolerance period makes the normal nodes attack the malicious nodes actively.

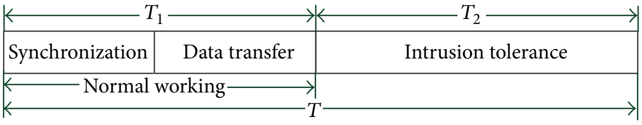


Figure 1: Time frame architecture 1.

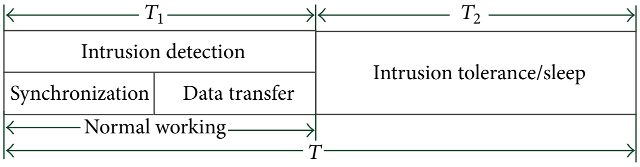


Figure 2: Time frame architecture 2.

To make the proposed method more effective, the normal working period implements the intrusion detection at the same time and the intrusion tolerance period can be changed with the sleep period, which is shown in Figure 2. In the initial state of the network, T_2 is the sleep period. When a normal node detects the presence of a malicious node, it will notify the sink node or the cluster head node to make all normal nodes change sleep period to intrusion tolerance period. As long as the malicious nodes exhaust their power, the normal nodes will be restored to its original time frame.

3.3.2. The Procedure of ITMEA. The detailed description of the process of ITMEA is as follows and the flow diagram of the process of ITMEA is shown in Figure 3.

Step 1. After the network initialization, the sink node sends intrusion tolerance command to the entire network. When the sensor node receives this command, it changes the original time frame architecture to time frame architecture 1 in Figure 1.

Step 2. When the normal working period ends, the sensor node i enters the intrusion tolerance period. The node i sets two timers T_{i1} and T_{i2} as well as the random waking times W_i which are determined by the number of malicious nodes in the network. When the number of the malicious nodes is uncertain, an initial value will be set. For example, $W_i = 3$. T_{i1} represents the total time of intrusion tolerance period and T_{i2} represents the sleeping time before the next wakeup of the node, satisfying $T_{i1} > W_i \cdot T_{i2}$.

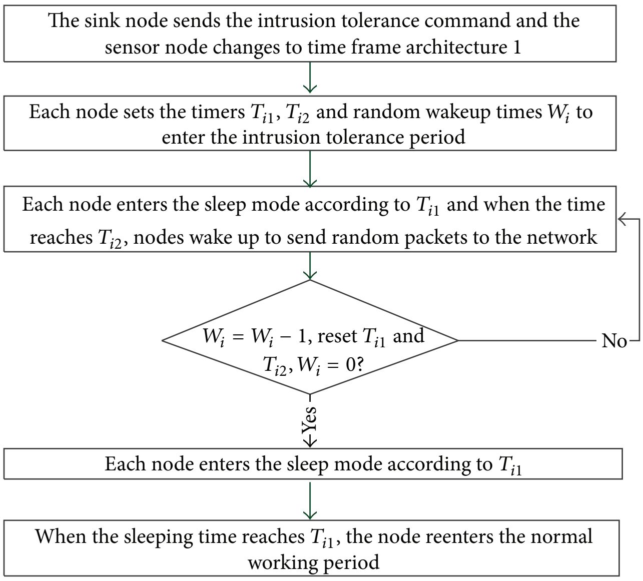

The sink node sends the intrusion tolerance command and the sensor node changes to time frame architecture 1
Each node sets the timers T_{i1}, T_{i2} and random wakeup times W_i to enter the intrusion tolerance period
Each node enters the sleep mode according to T_{i1} and when the time reaches T_{i2}, nodes wake up to send random packets to the network
$W_i = W_i - 1$, reset T_{i1} and T_{i2}, $W_i = 0$?
No
Yes
Each node enters the sleep mode according to T_{i1}
When the sleeping time reaches T_{i1}, the node reenters the normal working period

Figure 3: The flow diagram of ITMEA.

Step 3. At the beginning of intrusion tolerance period, the sensor node *i* shuts off the radio and MCU circuits to go into the power down mode and enters the sleep mode according to the T_{i1}. When the sleeping time reaches T_{i2}, the node *i* wakes up and turns on the TX and MCU circuits to transmit a random data packet D to the network. After transmitting the packet D, $W_i = W_i - 1$ and $T_{i1} = T_{i1} - T_{i2}$ will be set. The node recalculates T_{i2} which still satisfies $T_{i1} > W_i \cdot T_{i2}$, and T_{i1} and T_{i2} are set according to their new values.

Step 4. Step 3 is repeated until $W_i = 0$. Then the node *i* shuts off the radio and MCU circuits and enters the sleep mode according to T_{i1}.

Step 5. When the sleeping time reaches T_{i1}, the node reenters the normal working period.

3.3.3. The Usage of Intrusion Detection. The ITMEA method depicted in Figure 3 does not contain intrusion detection mechanism and the values of T_{i1}, T_{i2}, and W_i are set by the command from sink node. If there is no malicious node in the network, the transmission of random packets will waste the power of normal nodes. Therefore, the intrusion detection is applied in ITMEA, shorted as ITMEA_ID. The time frame architecture of ITMEA_ID has already been shown in Figure 2 and its process is slightly different from that of ITMEA. The ITMEA_ID adds some new mechanisms to the process as follows.

(1) If there is no malicious node detected, the normal nodes enter the sleep period instead of the intrusion tolerance period.

(2) The normal nodes detect the presence of malicious nodes and notify the sink node of the detected nodes. The sink node changes and sets the parameter values according to the reported number of the malicious nodes.

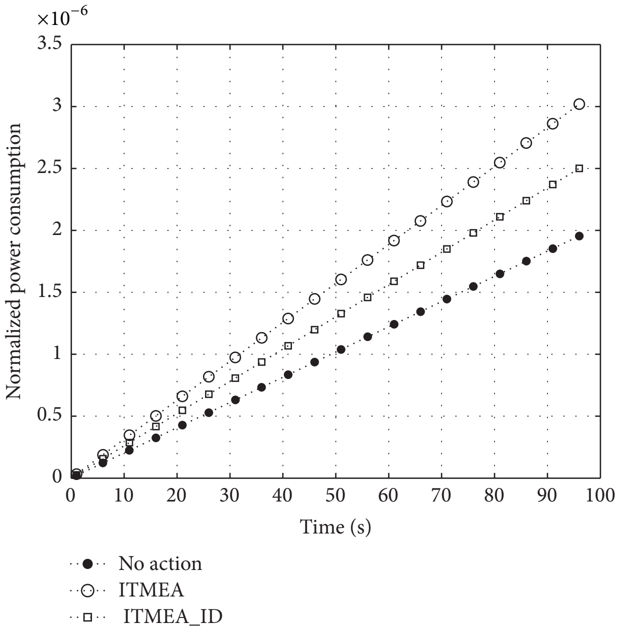


Figure 4: The power consumption of normal node with different methods.

(3) When the normal nodes detect that the malicious nodes exhaust their power to be useless, they notify the sink node and are set to enter the sleep period again.

Though the ITMEA_ID method saves power of sending invalid packets, the normal nodes have to implement intrusion detection which also consumes their limited power. A tradeoff between ITMEA and ITMEA_ID must be made to obtain a more effective method.

4. The Theoretical Analysis

To illustrate the effect of proposed methods, power consumption of the nodes needs to be quantified. By using CC2530 as the main chip of sensor node to run the simulations, current consumption of the four modes is listed in Table 1.

Firstly, power consumption of a sensor node with proposed methods is compared and ITMEA_ID uses the intrusion detection system architecture in [28]. The simulation parameters are listed in Table 3. Assuming that there is no malicious node in the network, the node using ITMEA_ID method will not enter the intrusion tolerance period. The normalized power consumption of node with different methods is shown in Figure 4. As seen from the figure, the power consumption of proposed methods is a bit higher than the node with no action. By applying parameters in Table 3, the original sensor node can last 579 days; the ITMEA_ID and ITMEA can last 463 days and 386 days, respectively. Therefore, applying the proposed intrusion tolerance method to the WSN is feasible.

Table 3: The simulation parameters.

T_1	T_s	T_d	T_2	T	T_{i1}[1]	T_{i2}[1]	W	Batt. power	Batt. vol.	Packet sending time
1 s	0.3 s	0.7 s	3 s	4 s	3 s	0.5 s	3	1500 mAh	1.5 V ∗ 2	1 ms

[1] T_{i1} and T_{i2} are the initial values.

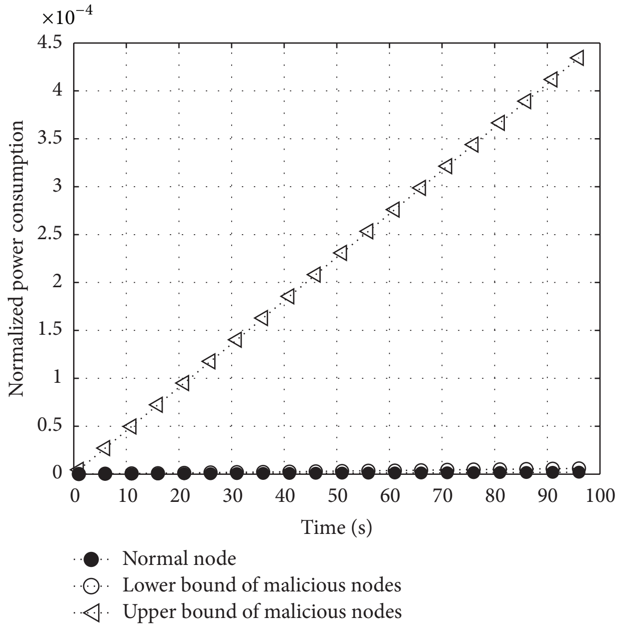


Figure 5: The power consumption of nodes without intrusion tolerance.

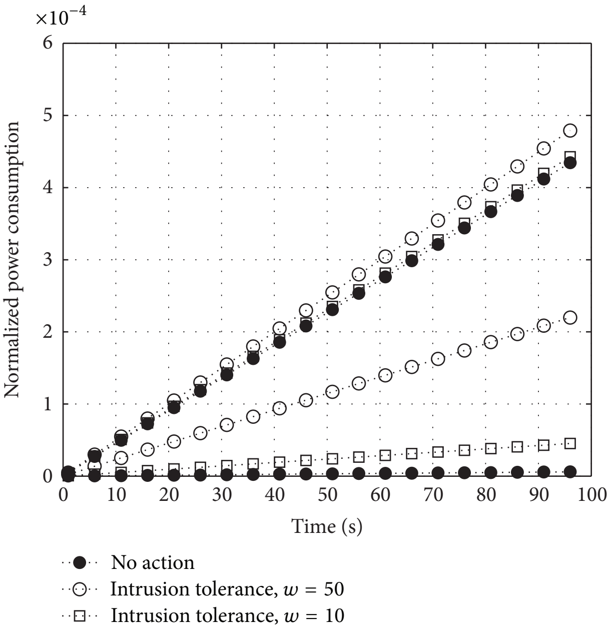


Figure 6: The power consumption bounds of malicious nodes.

Secondly, power consumption between the normal node and the malicious node is compared without the intrusion tolerance method. Assuming the malicious node just monitors the transmitting data but does not send any packet, the results can be obtained as shown in Figure 5. Monitoring consumes the least power of all attacks, so the curves in Figure 5 depict the least power consumption of a malicious node. The upper bound of the power consumption of a malicious node represents that the malicious node is in RX mode continuously and the lower bound represents that the malicious node is in RX mode during the packet sending and in sleep mode at the other time. Although the lower bound is conservative and ideal, it is very close to the curve of normal node, which means the malicious node will generate potential impact on the network for a long time. The practical power consumption of the malicious node is between the two bounds. The lower bound must be raised to decrease the lifetime of malicious node.

Thirdly, the proposed intrusion tolerance methods are used to increase the power consumption of malicious nodes. Because ITMEA_ID and ITMEA take the same actions in the intrusion tolerance period, the power consumption bounds of malicious node under the two methods are same. As shown in Figure 6, the bigger the value of W is, the higher the bounds will be. When $W = 50$, the lower bound increases significantly, which means the working time of malicious nodes decreases greatly.

Figure 7 shows the continuous working days of normal and malicious nodes which can monitor 4 neighbor nodes. As the value of W increases, the working days become fewer and the malicious nodes almost exhaust their power in only one day. However, the increase of W will also decrease the working days of normal nodes and the tradeoff must be made between the working time of the normal and malicious nodes. For example, as shown in the figure, when the value of W is about 50, the working days of the normal nodes are 100 and those of the malicious nodes are less than 5, which means that the normal nodes can spend five percent of its power to exhaust the energy of malicious nodes. After the death of malicious node, the ITMEA_ID method can decrease the value of W to extend the lifetime of normal nodes.

The number of normal nodes which malicious nodes can monitor also affects the power consumption of malicious nodes. The effects are shown in Figure 8 with $W = 10$. As the number of neighbor nodes increases, the working days of normal nodes using ITMEA are almost unchanged but those of normal nodes using ITMEA_ID decrease due to the intrusion detection mechanism. The increase of neighbor nodes reduces the working days of malicious nodes significantly, which makes the intrusion tolerance method freer. When the density of network is high, the sink node can command parts of normal nodes to enter the intrusion tolerance period to save power of the other nodes.

Theoretical simulations show that the proposed ITMEA and ITMEA_ID methods can exhaust the power of malicious

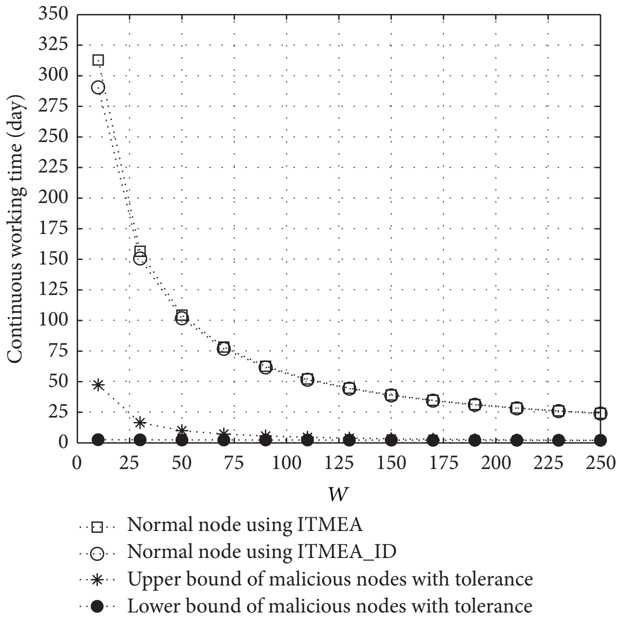


Figure 7: The continuous working days of the normal and malicious nodes, $N = 4$.

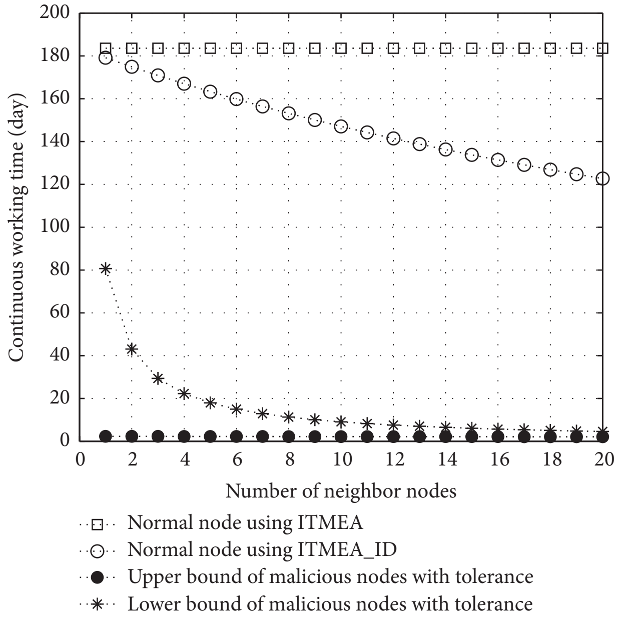


Figure 8: The continuous working days of the normal and malicious nodes, $W = 10$.

nodes rapidly and do not affect the normal functions and power consumption of normal network.

5. Test and Results Analysis

The performance of WSN based on the proposed intrusion tolerance methods is tested and analyzed in this section. The test system uses CC2530 to build the platform of sensor node. Some of the platforms are shown in Figure 9. The sensor nodes are configured with the parameters in Table 3 and the malicious nodes use the same platforms with normal nodes. The network with malicious nodes of different attacking methods runs about eight hours, respectively, and the results of average power consumption of sensor nodes are shown in Figure 10.

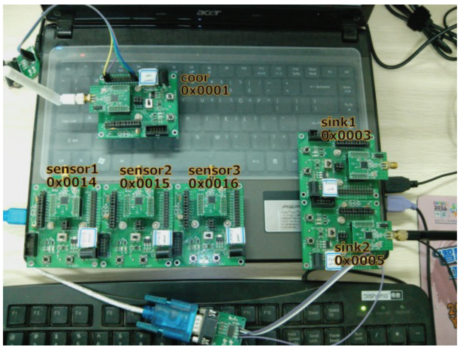


Figure 9: The platform of sensor nodes.

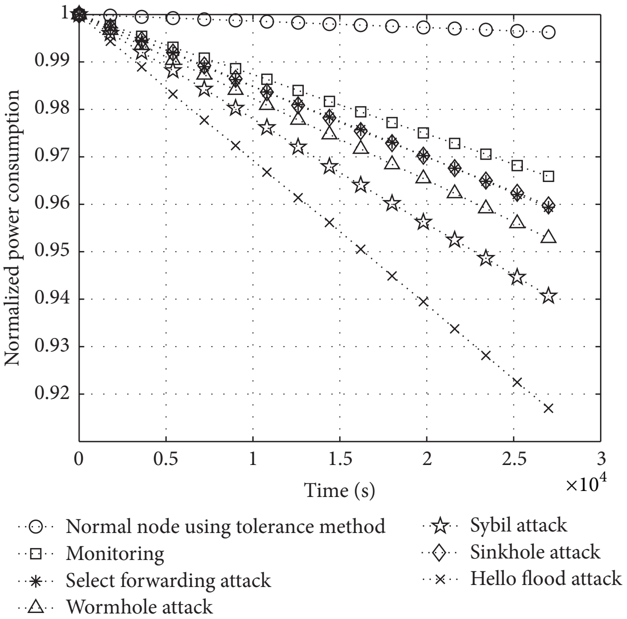


Figure 10: The power consumption of different attacks under intrusion tolerance.

The line with multiplication sign represents the average power consumption of a malicious node launching hello flood attack. In a hello flood attack, the malicious node sends as many data packets as possible to the entire network and its power consumption is the highest of all attacks.

The line with five-pointed star sign represents the average power consumption of a malicious node launching Sybil attack. The malicious node has several virtual identities, so it will communicate with different nodes of different identities. The power consumption increases with growth of the number of identities.

The line with triangle sign represents the average power consumption of a malicious node launching wormhole

Table 4: The continuous working days of malicious nodes.

	Monitoring	Select forwarding	Wormhole	Sybil	Sinkhole	Hello flood
Without tolerance	231.1	206.1	186.7	155.3	205.9	116.9
With tolerance	41.1	34.7	30.7	24.2	34.9	17.6

attack. In a wormhole attack, a malicious node replays the receiving packets to its partner and the power consumption increases with growth of the number of receiving packets.

The line with asterisk sign represents the average power consumption of a malicious node launching selective forwarding attack and the line with diamond sign represents the average power consumption of a malicious node launching sinkhole attack. As the two attacks use similar attacking method, the two curves show almost the same characteristics of power consumption.

The line with rectangle sign represents the average power consumption of a malicious node monitoring packets. The malicious nodes do not forward the receiving packets, so the power consumption is the least of all attacks.

As shown in Figure 10, the power consumption of different attacks in descending order is hello flood attack > sybil attack > wormhole attack > sinkhole attack ≈ select forwarding attack > monitoring. The continuous working days of malicious nodes with different attacks are calculated by the collected sampling data of power consumption. The data of the malicious nodes without intrusion tolerance are also collected and calculated, which are shown in Table 4.

The sensor nodes are configured with the same parameters and working conditions as in Table 4 and the changes of working days show the efficiency of proposed methods. The continuous working days of malicious nodes decrease significantly with intrusion tolerance methods.

6. Conclusions and Future Work

Different from the traditional intrusion tolerance methods, the ITMEA and ITMEA_ID are proposed with the mechanism of attacking malicious nodes actively. Relative to the three kinds of intrusion tolerance techniques in Section 2, the active protection method uses different security policy and requires very little resource overhead. The main advantages and differences are as follows.

(1) For the malicious nodes, the proposed methods can decrease the lifetime of malicious nodes whose attacking time will be far below their normal lifetime. The active protections exhaust the power of malicious nodes to make the network return to normal state. However, the existing methods will live with the malicious nodes during their normal lifetime, which may generate a serious impact.

(2) The security protocol method has to establish protocols and interact among them; the redundancy management method needs redundancy resources; and the trust model requires reputation-based frameworks. All of these methods are more suitable to be applied in resource-rich environment. The proposed method consumes less resource as its main consumption occurs in synchronization and intrusion tolerance period.

(3) For the normal nodes, as the increase of the network size, the network power consumption of security protocol and trust mode methods keeps increasing regardless of the number of malicious nodes, but that of the proposed methods is decided by the number of malicious nodes.

(4) The proposed methods show different performance to different attacks and the hello flood and Sybil attack are especially vulnerable.

The proposed methods exchange small power consumption of many normal nodes for large power consumption of relatively small number of malicious nodes to decrease the lifetime of malicious nodes. The ITMEA_ID adds intrusion detection to the ITMEA, which improves the efficiency of method but increases the power consumption during intrusion detection and the combination of the two methods makes a tradeoff.

The theoretical analysis and test results show that the proposed methods not only prolong the lifetime of sensor network but also achieve the effective protection against malicious nodes. More neighbor nodes and longer tolerance period will yield better tolerant performance, so the proposed methods are more suitable for a dense network or applications without hard time constrains. WSNs with ITMEA can be deployed for both civil and military applications which typically work in harsh environments and examples of practical applications include area monitoring, environmental sensing, agricultural control, industrial monitoring, and military surveillance.

For future work, we plan to simplify the synchronization protocol and optimize configuration of parameters in the proposed method by practical experiments and also we will plan to explore more extensive attacks to increase the applicability of the method.

Conflict of Interests

The authors declare that they have no conflict of interests.

Acknowledgments

This work is funded by the National High Technology Research and Development Program of China (863 Program) under Project no. 2013AA014001, the National Science & Technology Pillar Program, supported by the Ministry of Science and Technology of People's Republic of China under Contract no. 2012BAH38B05, and the Cooperative Innovation Center of 2011. The authors would like to thank the editor and anonymous reviewers for their invaluable comments and suggestions.

References

[1] M. Tubaishat and S. K. Madria, "Sensor networks: an overview," *IEEE Potentials*, vol. 22, no. 2, pp. 20–23, 2003.

[2] S. Panichpapiboon, G. Ferrari, and O. K. Tonguz, "Optimal transmit power in wireless sensor networks," *IEEE Transactions on Mobile Computing*, vol. 5, no. 10, pp. 1432–1447, 2006.

[3] M. Whitman and H. Mattord, *Principles of Information Security*, Cengage Learning, 2011.

[4] J. Fraga and D. Powell, "A fault-and intrusion-tolerant file system," in *Proceedings of the 3rd International Conference on Computer Security*, pp. 203–218, 1985.

[5] A. Perrig, R. Szewczyk, J. D. Tygar, V. Wen, and D. E. Culler, "SPINS: security protocols for sensor networks," *Wireless Networks*, vol. 8, no. 5, pp. 521–534, 2002.

[6] S. Zhu, S. Setia, and S. Jajodia, "LEAP+: efficient security mechanisms for large-scale distributed sensor networks," *ACM Transactions on Sensor Networks*, vol. 2, no. 4, pp. 500–528, 2006.

[7] T. Park and K. G. Shin, "LiSP: a lightweight security protocol for wireless sensor networks," *ACM Transactions on Embedded Computing Systems*, vol. 3, no. 3, pp. 634–660, 2004.

[8] C. Karlof, N. Sastry, and D. Wagner, "TinySec: a link layer security architecture for wireless sensor networks," in *Proceedings of the 2nd International Conference on Embedded Networked Sensor Systems (SenSys '04)*, pp. 162–175, November 2004.

[9] M. Luk, G. Mezzour, A. Perrig, and V. Gligor, "MiniSec: a secure sensor network communication architecture," in *Proceedings of the 6th International Symposium on Information Processing in Sensor Networks (IPSN '07)*, pp. 479–488, April 2007.

[10] A. Liu and P. Ning, "TinyECC: a configurable library for elliptic curve cryptography in wireless sensor networks," in *International Conference on Information Processing in Sensor Networks (IPSN '08)*, pp. 245–256, April 2008.

[11] L. Casado and P. Tsigas, "Contikisec: a secure network layer for wireless sensor networks under the contiki operating system," in *Identity and Privacy in the Internet Age*, Springer, 2009.

[12] D. Jinwala, D. Patel, and K. Dasgupta, "FlexiSec: a configurable link layer security architecture for wireless sensor networks," *Journal of Information Assurance and Security*, vol. 4, pp. 582–603, 2009.

[13] N. Bandirmali and I. Erturk, "WSNSec: a scalable data link layer security protocol for WSNs," *Ad Hoc Networks*, vol. 10, no. 1, pp. 37–45, 2012.

[14] Y.-T. Tsou, C.-S. Lu, and S.-Y. Kuo, "MoteSec-aware: a practical secure mechanism for wireless sensor networks," *IEEE Transactions on Wireless Communications*, vol. 12, no. 6, pp. 2817–2829, 2013.

[15] J. Deng, R. Han, and S. Mishra, "INSENS: intrusion-tolerant routing for wireless sensor networks," *Computer Communications*, vol. 29, no. 2, pp. 216–230, 2006.

[16] J. Deng, R. Han, and S. Mishra, "Intrusion tolerance and anti-traffic analysis strategies for wireless sensor networks," in *Proceedings of the International Conference on Dependable Systems and Networks*, pp. 637–646, IEEE, July 2004.

[17] H. Al-Hamadi and I.-R. Chen, "Redundancy management of multipath routing for intrusion tolerance in heterogeneous wireless sensor networks," *IEEE Transactions on Network and Service Management*, vol. 10, no. 2, pp. 189–203, 2013.

[18] A. Hemalatha and R. Venkatesh, "Redundancy management in heterogeneous wireless sensor networks," in *Proceedings of the International Conference on Communications and Signal Processing (ICCSP '14)*, pp. 1849–1853, Melmaruvathur, India, April 2014.

[19] M. Wei and K. Kim, "Intrusion tolerance mechanisms using redundant nodes for wireless sensor networks," in *Proceedings of the 28th International Conference on Information Networking (ICOIN '14)*, pp. 131–135, IEEE, Phuket, Thailand, February 2014.

[20] S. Ganeriwal, L. K. Balzano, and M. B. Srivastava, "Reputation-based framework for high integrity sensor networks," *ACM Transactions on Sensor Networks*, vol. 4, no. 3, article 15, 2008.

[21] L. Huang and L. Liu, "Extended watchdog mechanism for wireless sensor networks," *Journal of Information and Computing Science*, vol. 3, no. 1, pp. 39–48, 2008.

[22] D. He, C. Chen, S. Chan, J. Bu, and A. V. Vasilakos, "ReTrust: attack-resistant and lightweight trust management for medical sensor networks," *IEEE Transactions on Information Technology in Biomedicine*, vol. 16, no. 4, pp. 623–632, 2012.

[23] X. Li, F. Zhou, and J. Du, "LDTS: a lightweight and dependable trust system for clustered wireless sensor networks," *IEEE Transactions on Information Forensics and Security*, vol. 8, no. 6, pp. 924–935, 2013.

[24] G. Zhan, W. Shi, and J. Deng, "SensorTrust: a resilient trust model for wireless sensing systems," *Pervasive and Mobile Computing*, vol. 7, no. 4, pp. 509–522, 2011.

[25] F. Bao, I.-R. Chen, M. Chang, and J.-H. Cho, "Hierarchical trust management for wireless sensor networks and its applications to trust-based routing and intrusion detection," *IEEE Transactions on Network and Service Management*, vol. 9, no. 2, pp. 169–183, 2012.

[26] T. Martin, M. Hsiao, D. Ha, and J. Krishnaswami, "Denial-of-service attacks on battery-powered mobile computers," in *Proceedings of the 2nd IEEE Annual Conference on Pervasive Computing and Communications (PerCom '04)*, pp. 309–318, March 2004.

[27] W. Ye, J. Heidemann, and D. Estrin, "An energy-efficient MAC protocol for wireless sensor networks," in *Proceedings of the 21st Annual Joint Conference of the IEEE Computer and Communications Societies (INFOCOM '02)*, pp. 1567–1576, June 2002.

[28] R. Roman, J. Zhou, and J. Lopez, "Applying intrusion detection systems to wireless sensor networks," in *Proceedings of the 3rd IEEE Consumer Communications and Networking Conference (CCNC '06)*, vol. 1, pp. 640–644, January 2006.

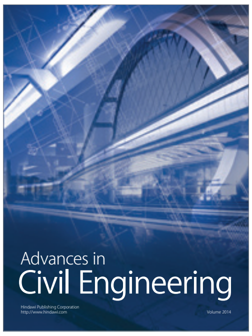
Journal of
Engineering

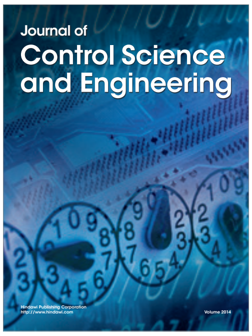
The Scientific
World Journal

International Journal of
Rotating
Machinery

Journal of
Sensors

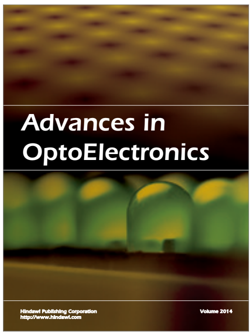
International Journal of
Distributed
Sensor Networks


Advances in
Civil Engineering


Journal of
Control Science
and Engineering

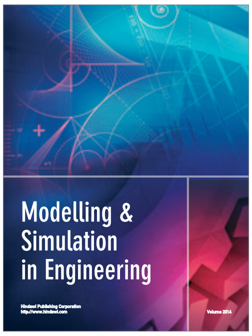
Journal of
Robotics

Journal of
Electrical and Computer
Engineering

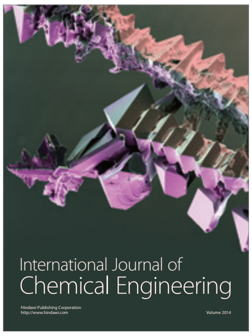

Advances in
OptoElectronics

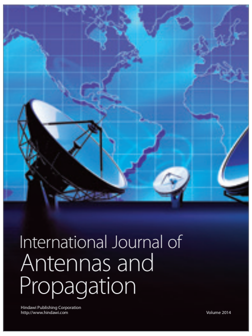
VLSI Design

International Journal of
Navigation and
Observation

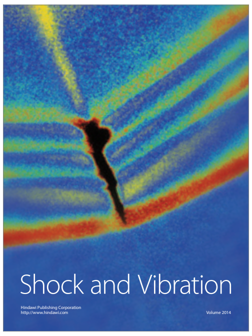

Modelling &
Simulation
in Engineering

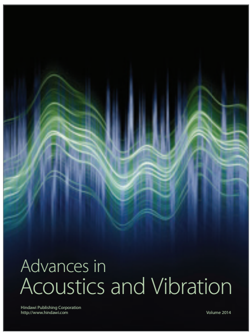
International Journal of
Aerospace
Engineering


International Journal of
Chemical Engineering


International Journal of
Antennas and
Propagation

Active and Passive
Electronic Components


Shock and Vibration


Advances in
Acoustics and Vibration