http://ansinet.com/itj

ITJ

ISSN 1812-5638

# INFORMATION TECHNOLOGY JOURNAL

ANSInet
Asian Network for Scientific Information
308 Lasani Town, Sargodha Road, Faisalabad - Pakistan

Information Technology Journal 12 (9): 1764-1771, 2013
ISSN 1812-5638 / DOI: 10.3923/itj.2013.1764.1771


# An Intrusion Detection System for Cluster Based Wireless Sensor Networks

[1]Xue Deng, [2]Renyong Wu, [2]Wenru Wang and [2]Renfei Bu
[1]Key Laboratory for Embedded and Network Computing of Hunan Province,
Changsha, Hunan, 410082, People's Republic of China
[2]School of Information Science and Engineering, Hunan University, Changsha, China

**Abstract:** With the rapid development of wireless communication technology, wireless sensor networks (WSNs) have been widely used in many fields. Therefore, the security become an important issue in WSNs. Compared with the wired network, wireless sensor networks have its own features. The one is limited resource, such as energy, computing power and communication capability. The other is attack types. There are some additional attacks appear on sensor node, such as node capture and tampering. As a result,the security mechanisms which work well in wired network can not be applied in wireless senor network directly. In this paper, in order to improve the security level of WSNs, we proposed a new intrusion detection system (IDS) to find malicious node in WSNs. According to the deviation from the normal pattern of node's behavior, basic input vector of evidence is constructed. Furthermore, the weight value is applied to represent the importance of each behavior characteristic and revise the evidence before evidence synthesis. Finally, by utilizing evidence theory and judgment rules, the running state of the evaluated node is obtained. Extensive simulation results show that the proposed IDS is more effective in detecting malicious nodes than existing schemes.

**Key words:** Wireless sensor networks, security, intrusion detection system, behavior characteristic, evidence theory, weight algorithm

## INTRODUCTION

In general, Wireless Sensor Networks (WSNs) consist of a large number of small-size, energy-constrained nodes, it is a kind of wireless communication network. The main function of WSN is to collect data samples from the monitoring area and forward the sensed data to the base station (Akyildiz *et al*., 2002). With the rapid development of Information Technology (IT), WSNs have been widely used in many fields. In military applications, WSNs are often deployed in battlefield to monitor the movements of enemy so as to provide effective reference information for army. As for industrial production, WSNs play a huge role in production safety, such as the monitoring of nuclear power plants operation and so on (Lu and Xue, 2010).

However, due to the application needs, the sensor nodes are often distributed in harsh or hostile environment for a long time which makes them easy to be attacked by intruder. As a result, the security is an important issue while WSNs are widely used. Although some prevention mechanisms is established to deal with well-know attacks, it cannot resist all kinds of attacks. Therefore, in order to increase the security level of WSNs, it is necessary to propose a reasonable and applicable intrusion detection system for WSNs (Alemdar and Ibnkahla, 2007; Zhou *et al*., 2008).

As we all know, flat WSN and Cluster based WSN (CWSN) are two most common topologies of WSNs (Yang *et al*., 2012). Because of efficient energy utilization and strong scalability, CWSN is more widely used. The topology of CWSN can be seen from Fig. 1. As shown in Fig. 1, CWSN contain three kinds of nodes. The first kind of node is named Sensor Node (SN) which is responsible for data sensing. As these SNs are equipped with limited resource and are intensively distributed in monitoring area, they are the main target of attack. The second kind of node is named Cluster Head (CH). After receiving the data packet from SNs, the CHs first filter abnormal data and then transmit the filtered data to BS. In our IDS, CHs have more energy and computing power than SNs, the CHs in IDS are used to detect the malicious SNs in its cluster. The third kind of node is called Base Station (BS) which integrates the whole collected information and transmits the final result to user.

As the name suggests, intrusion detection system is a technology to detect the intrusion which attempt to destruct the normal operation of network by tampering with the data, intercepting data, changing the direction of data transmission or other illegal methods. Intrusion

**Corresponding Author:** Renyong Wu, School of Information Science and Engineering, Hunan University, Changsha, 410082 China

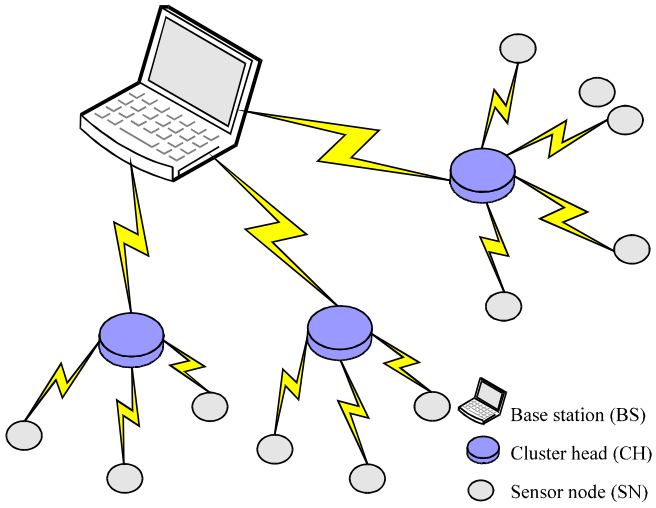


Fig. 1: Topology of cluster based wireless sensor networks

detection system is a real-time monitoring of network transmission. When a sensor node is detected as malicious node, it will be isolated from the network. By this way, the reliability of sensed data can be ensured.

The method of intrusion detection system can be divided into two parts: misuse detection and anomaly detection (Depren *et al*., 2005). In misuse detection system, the well-know attack behavior characteristics are first constructed into database and then make a comparison between the monitored behavior and database. If the monitored behaviors are similar to the rules recorded in database, the misuse detection system will define the evaluated node as malicious node. The biggest advantage of misuse detection system is that it can detect common types of attack which is included in database with high detection ratio and low misdetection ratio. However, the main drawback of misuse detection system is that it cannot identify novel attack behaviors which are not recorded in database. What's worse, if taking the measure of update node database through network, it will bring too much additional consumption which will not well adapt to the requirement of low energy consumption in intrusion detection system.

As to anomaly detection method, system defines exactly the normal nodes' behavior characteristic and then report the nodes which have big different from normal level. This method can deal with new attack types. However, the misdetection ratio of anomaly detection method is higher than misuse detection system. The reason why is that the monitoring environmental changes quickly, it is difficult to distinguish between normal behavior and malicious behavior. So, the normal node will often be misjudged as malicious node.

In order to address these issues mentioned above, in this study, we proposed a new intrusion detection system based on weight and evidence theory to detect the malicious nodes in CWSN. The main contributions of this paper can be summarized as follows:

- Multi-dimension method is adopted to collect the behavior characteristic of the evaluated node. Most of the attacks which influence one or more aspects of node behavior can be correctly detected
- Evidence theory and weight algorithm is used to build the architecture of proposed intrusion detection system in this paper which will accurately reflect the real situation of the evaluated node
- Extensive simulation results show that our approach is more effective in detecting malicious nodes with high detection ratio and low misdetection ratio at the same time

## RELATED WORK

In recent years, there have appeared some research works on intrusion detection system for WSNs. (Zhang and Lee, 2000) proposed an IDS for distributed wireless networks. In their scheme, they use local detection engine to identify malicious nodes in network. If the running state of evaluated node cannot be determined by local detection engine, the network will launch a cooperative intrusion detection procedure to

help local analysis. This method is simple and easy to understand, but it will consume much time and energy to exchange local detection information between nodes.

Ribeiro *et al*. (2004) introduce an IDS depend on neighbor node detection. In their scheme, they detect a malicious node based on signal strength. When the value of Received Signal Strength Indicator (RSSI) detected by evaluation node is does not match to the local preset value, the evaluated node will be marked as malicious node. Even though this approach is applicable, it is not efficient in many ways. The RSSI is great influence by environment factors, only from the RSSI value to determine the running status of the evaluated node will result in a high rate of misdetection.

Hu *et al*. (2003), Tumrongwittayapak and Varakulsiripunth (2009) and Moon and Cho (2009) proposed an IDS for specified attacks, such as sinkhole attack, selective forwarding attack etc. These IDS are designed according to specified attack features, so these IDS have good performance as to the specified attack. When the network suffer from multiple attacks at the same time, the IDS in their study are not enough to ensure the security of network.

To defend many types attack (Haddadi and Sarram, 2010) introduce an agent-based IDS, the agent node monitors the wireless network on multiple channels and uses three engines to detect different type of intrusions. The structure of this IDS is reasonable, but it requires the introduction of agent node which will increase the cost.

The study reported by Chang and Liu (2011) proposed an IDS based on evidence theory. By using the evidence theory to merge the monitored behavior characteristics, the proposed IDS output a comprehensive assessment result which can reflect the security of the evaluated node. This scheme is similar to our paper in some degree. However, it does not take the reliability of each behavior characteristic into consideration.

In this study, we present an applicable and efficient IDS for CWSN. In order to defend many types attack, the proposed detection model collects the multi-dimension behavior characteristic from evaluated node. Then the evidences are constructed according to the deviation of behaviors from normal level. Weigh mechanism is used to represent the reliability of evidence and revise evidence before evidence confusion. Finally, through evidence theory synthesis and judgment rules, we get the output of IDS. By using the proposed IDS, malicious nodes in CWSN can be found out correctly and the overall performance of network will be improved.

## PRELIMINARY

Before elaborate our IDS, we first briefly introduce the fundamental concepts of Dempster-Shafer (D-S) evidence theory and weight theory here which are the theoretical basis of our intrusion detection system.

**D-S evidence theory:** D-S evidence theory (Dempster, 1967; Shafer, 1976) is a method of uncertainty reasoning which was first proposed by Dempster (1967) and then further developed by his student Shafer (1976). The theory can be seen as generalized broaden of classical probabilistic inference theory in finite fields and support probabilistic inference, probabilistic diagnosis, risk analysis and decision support. What's more, evidence theory can clearly express the uncertainty and effectively deal with uncertain information in case of no prior information.

**Frame of discernment and assignment function:** If all possible outcomes for an issue of jurisdiction are regarded as a set, this complete set is called a frame of discernment ($\Theta$).

Based on the frame of discernment, mapping $m:2^{\Theta}\rightarrow[0,1]$ ($2^{\Theta}$is the power set of $\Theta$) is called as Basic Probability Assignment function (BPA) and it meets the following requirements:

$$\begin{cases} m(\varnothing)=0 \\ \sum_{i=1}^{n} m(A_i)=1, A_i \subseteq \Theta \end{cases} \quad (1)$$

where, $\varnothing$ is denote empty set. If $m(A)>0$, $A_i$ is called as focal element.

In our IDS, the frame of discernment $\Theta$ is defined as {T,-T} and power set $2^{\Theta}$ is {$\Phi$, {T}, {-T}, {T, -T}}, represent empty set, the state of evaluated node's normal state, abnormal state and uncertain state. In order to express convenience, we marked these three running state with $T_1$, $T_2$, $T_3$, respectively.

**Belief function and plausibility function:** The belief function (Bel) and Plausibility Function (Pl) are two decision criteria. Bel(A) shows the true trust level of focal element A. Pl(A) reflects the maximum or potential support for focal element A. These two measures are defined as a map from a set of focal element to interval [0, 1] as follows:

$$Bel(A)=\sum_{B\subseteq A} m(B) \quad (2)$$

$$Pls(A)=\sum_{B\cap A\neq\varnothing} m(B) \quad (3)$$

**Dempster synthesis rule:** The main function of synthesis rules in evidence theory is to fuse multiple information sources and output a new basic probability assignment. Assume that there are n BPA functions $m_1$, $m_2$, $m_3$ which come from the same frame of discernment. The synthesis rule is:

$$m(A)=\begin{cases}0, & A=\varnothing\\ \dfrac{1}{1-K}\sum_{\cap A_i=A}\prod_{1\le i\le n} m_i(A_i), & A\neq\varnothing\end{cases} \quad (4)$$

And:

$$K=\sum_{\cap A_i=\varnothing}\prod_{1\le i\le n} m_i(A_i) \quad (5)$$

where, K is the measure of conflict between the different information and it is introduced as a normalization factor.

It is note that the credibility of all the evidences is equal in the synthesis process in Eq. 4. However, in practical applications, because uncontrollable environmental factors or nodes' own reasons often makes the important of different behavior characteristic is not the same. To solve this problem, we introduce a weight mechanism which revises the input evidence according to the weight value of evidences before synthesis. The calculation process of weight value will be discussed later.

**Weight theory:** The weighting algorithm is vital to combination and decision process of multi-dimensional information because its output will directly reflects each factor's important and position in the final results (Chen *et al*., 2005). In the process of fusion, assume there are n attributes in system and the $\omega_i$ attribute's weight is denoted as $\omega_i$. Then, all the weight values subject to:

$$\omega_1+\omega_2+L+\omega_n = 1 \quad (6)$$

The main strategies of weighting algorithm include expert evaluation method, fuzzy statistics and duality contrast sorted method, etc. Its shortage lies in that, if the weight values are determined by expert experience, they cannot objectively reflect the actual circumstance and sometimes even result in a false in evaluation and decision-made process. Therefore in this study, the weight value of evidences is obtained according to history record. By analyzing the contribution record of evidence in historical judgment, each evidence will be allocated a reasonable weight value. As a result, it will lead to a more accurate final output than under the situation that weight values only depend on the experience knowledge.

## ARCHITECTURE OF THE PROPOSED IDS

In this section, we present our IDS in detail and explain how the IDS works. The proposed IDS in this study is suitable for CWSN, in which CHs will act as evaluator to make an assessment on Sns in its cluster. In our IDS, we assume that the CHs and BS will not be compromised. The implementation of IDS embedded in Chs consists of five steps:

- **Step 1:** Collection of SN's behavior characteristic. It is well know that different types of attack will have different effect on nodes' behavior. In order to resist different attacks, a multi-dimension behavior characteristic collection method is adopted in this paper. Here, the CHs collect the behavior characteristic of SNs from four aspects

**Energy consumption (EC(t)):** The total energy consumption of the evaluated SN within a monitoring cycle:

$$EC(t) = R(t-\Delta r)-R(t) \quad (7)$$

where, R(t) denote the remaining energy of SN at time t. $\Delta t$ is the monitoring time period.

**Packet sending number (PSN(t)):** The number of sending packets of evaluated SN within a monitoring cycle. In WSNs, all sensor nodes send packet by means of broadcast, so the packet send by SN can be received by its CH. What's more, different SN in the network has a different ID and this information will add to the head of packet when it sent. By analysis the received packet of CH, the number of sending packets of the evaluated SN can be statistical.

**Packet loss number (PLN):** The relativity between hello packets sent to the evaluated SN and ACK feedbacks received by CH. In WSNs, ACK mechanism is widely used to assure the reliable transmission of packet. When

a sensor node received a packet from other node, it will send back a confirmation packet to the node which sends the packet to it. This confirmation packet is called as ACK packet:

$$PLN(t) = S(t)\text{-}N_{ACK}(t) \quad (8)$$

where, S(t) is the total number of packets that send to the evaluated SN and $N_{ACK}$ is the number of ACK packets received by corresponding CH.

**Data consistency (DC(t)):** The consistency of the evaluated SN sensed data with the rest of nodes in its cluster. Because the wireless sensor nodes are densely distributed in the monitoring area, the sensed data in the same cluster will have a high degree of similarity. By comparing the data sensed by the evaluated SN with that of other cluster member nodes, we can determine whether the evaluated SN has modified the sensed data. If the difference of sensed data between the evaluated SN and the cluster member node is less than 20%, we think that sensed data has not be modified. Otherwise, the sensed data by the evaluated SN will be considered as inconsistent data packet. During each monitoring period, the CH record the number of inconsistency data packet which send by the evaluated SN.

- **Step 2:** Calculate the deviation value of collected behavior characteristic. When the network is initialized, the network is often running in a normal state, we first monitor the whole network for a long time and then get the expected value of the evaluated SN's behavior characteristic. After that, the deviation value of collected behavior characteristic and expected value can be calculated as follows:

$$d = \frac{|C - E|}{E} \quad (9)$$

where, C is the value of collected behavior characteristic (EC, PSN, PLN, DC) and E is the corresponding expected value.

- **Step 3:** Pretreatment and constructing the input evidence vector. In order to reduce the computational complexity, we first preprocess the obtained deviation value. If any deviation value of the evaluated SN's collected behavior characteristic is more than 50%, the evaluated SN will be judged as malicious node directly. Otherwise we put the deviation value of collected behavior characteristics to designed BPA function and get 4 input evidence vectors

From the evidence theory we know that the design of BPA function should follow two basic principles. First, the summation of all BPA function must be 1. Second, the BPA value of $T_1$, $T_2$, $T_3$ should meet: The bigger the deviation value is, the greater the likelihood of malicious the evaluated SN are. Based on the two basic principles mentioned above, the formula of BPA function can be built as follows:

$$\begin{cases} m(T_1) = \dfrac{1 - 2d}{1.52 - 0.52|1 - 4d|} \\ m(T_2) = \dfrac{2d}{1.52 - 0.52|1 - 4d|} \\ m(T_3) = \dfrac{0.52 - 0.52|1 - 4d|}{1.52 - 0.52|1 - 4d|} \end{cases} \quad (10)$$

It is note that, when d = 50%, $m(T_1) = 0$, $m(T_2) = 1$, $m(T_3) = 0$, it is means the evaluated SN is a malicious node.

- **Step 4:** Calculate the weight value. In order to overcome the dependence of person's subjective judgment, in this study, the weight value is determined by each behavior characteristics' history contribution. In each round of detection, the CH records the result of judgment and builds a decision table to identify the evidence which is the largest contribution to this result. It should be noted that, in our IDS, each evidence is obtained by the deviation value of behavior characteristic. So, the difference sequence number of evidence ($m_i$) represents the different behavior characteristic of evaluated SN. An example of decision table can be seen in Table 1

In Table 1, the final detection result of evaluated SN is state $T^1$ which means the evaluated SN is a normal node. Obviously, from the table we know that the third evidence is the most support such a judgment. Then, we define the contribution value of third evidence plus 1.Under this method, we use the sliding window to statistic the contribution value of each evidence in recent 6 detection round. A sample scenario of sliding window is illustrated in Fig. 2.

Table 1: An example of decision table BPA: Basic Probability Assignment

| BPA value | $T_1$ | $T_2$ | $T_3$ | Detection result |
|---|---|---|---|---|
| $m_1$ | 0.65 | 0.30 | 0.05 | $T_1$ |
| $m_2$ | 0.73 | 0.16 | 0.11 | |
| $m_3$ | 0.82 | 0.06 | 0.12 | |
| $m_4$ | 0.62 | 0.17 | 0.21 | |

$T_1$: The normal running state of evaluated node, $T_2$: The abnormal running state of evaluated node, $T_3$: The uncertain running state of evaluated node $m_i$: The inputted evidence

In the Fig. 2, the sequence number of most contribution evidence in each detection round are recorded in the window. After a round of detection, the window slides one unit to the right, thereby dropping the record in the first unit. Thus, as time progresses, the window forgets the experiences of one unit but adds the experiences of the newer one. From Fig. 2 we know that, the sequence number of evidence named 1 have 3 times contribution in recent 6 detection round and evidence 2 has 2 times, evidence 3 has 1 times, evidence 4 has 0 times, respectively. Then according to the contribution value, the weight value of each evidence is obtained. To the evidence which has no obviously contribution in recent judgment, just like evidence 4, we define its weight value as 0.1 according to expertise. The weight value of other evidences can be calculated as follows:

$$\omega_i = \begin{cases} 0.1 & ,g = 0 \\ \dfrac{(1-0.1\times n)\cdot g}{\sum g} & ,g \neq 0 \end{cases} \quad (11)$$

where, g is the contribution value of corresponding evidence. N is the total number of evidences which have no obviously contribution in recent 6 detection round.

- **Step 5:** Evidence synthesis and judgment. After obtained the weight value of each evidence, we will focus now on how to integrate these evidences. First, we integrate all the evidences based on the weight value and get the desired evidence:

$$M(T_j) = \sum_{i=1}^{4} w_i m_i(T_j), j = 1,2,3 \quad (12)$$

Then, we use the desired evidence to iterative integration for 3 times according to Eq. 4 and output the synthesis result.

Finally, the judgment unit output the running state of evaluated SN by analyzing the synthesis result. If the synthesis results satisfy:

$$\begin{cases} Bel(T_1) < 0.25 \\ Bel(T_2) > Pl(T_1) \end{cases} \quad (13)$$

The evaluated SN will be marked as malicious node and its ID will be list in blacklist. Otherwise, the evaluated SN will be classified to the state which is the synthesis result most support.

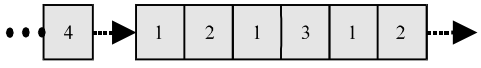


Fig. 2: An example of sliding window

## SIMULATION RESULTS

**Simulation setting:** We evaluated the proposed IDS through a simulation system developed by JAVA. The simulation scene is show in Fig. 3. Simulation system consists of 1000 sensor nodes. To make the simulation more realistic, these nodes are randomly deployed over a square area of 400×400 m meters. All malicious nodes are randomly selected and run with one or more types attack, e.g., denial of service attack (Dos), flooding attack or other anomaly behaviors. Further specifications of simulation parameter are defined in Table 2.

**Performance evaluation:** There are many standards measure the performance of IDS. Here, we compare our scheme with WTA (Ju *et al*., 2010) from two major aspects: Detection Ratio and Misdetection Ratio.

The detection ratio is defined as the percentage of malicious nodes that are successfully detected out of the whole malicious nodes. It is the main criteria to measure the performance of an IDS. The higher the detection ratio value, the better the performance of IDS. The detection ratio of our IDS and WTA can be seen in Fig. 4.

Table 2: Parameter values in simulation

| Parameters | Values |
|---|---|
| Simulation times (sec) | 1000 |
| Percent of malicious nodes (%) | 25 |
| Detection interval (sec) | 10 |
| Transmission radius (m) | 10 |
| Packet data (byte) | 512 |
| Initial energy (J) | 10 |
| Initial state of node | Normal |

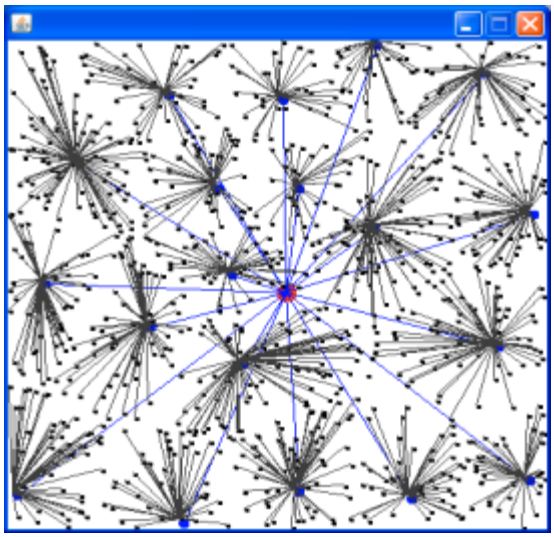

Fig. 3: Simulation scenario

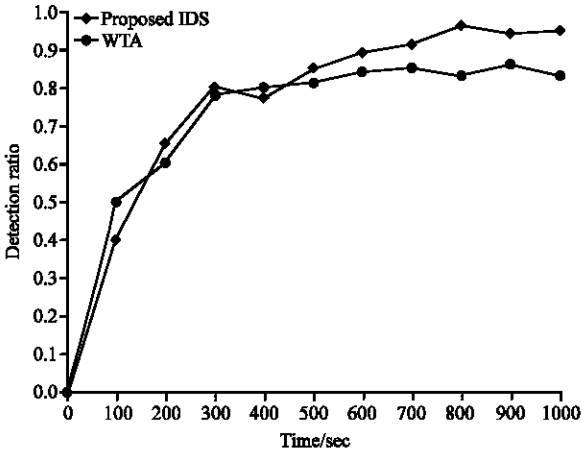


Fig. 4: Compared the detection ratio performance, WTA: Weight-trust application scheme

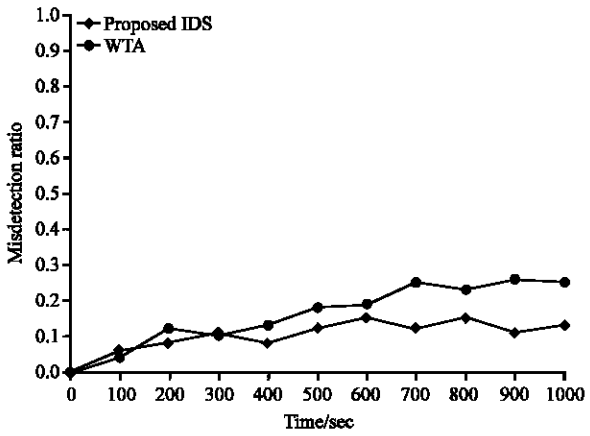


Fig. 5: Compared the misdetection ratio performance, WTA: Weight-trust application scheme

As shown in Fig. 4, both the detection ratio of our IDS and WTA are increased over time. However, the detection ratio of proposed IDS is higher than WTA after 500 sec. The reason for this phenomenon can be explained from two aspects. On one hand, with the passage of time, the number of detection round increased, so both detection ratios have increased. On the other hand, in our IDS the weight value of each behavior characteristic is obtained by history contribution which will cause malicious behavior more prominent and easy to be detected. However, in WTA the weight value is getting only by the number of abnormal data in history communication. When the network suffers from some attacks which didn't tamper the data, WTA cannot detect it out correctly.

The misdetection ratio is claimed as the ratio between the number of misjudged nodes and the number of correctly detected malicious nodes. Specifically, the number of misjudged nodes consists of two parts: the one is the number of normal nodes which are misjudged as malicious nodes. The other is the number of malicious nodes which are misjudged as normal nodes. Figure 5 shows the misdetection ratio of proposed IDS and WTA.

In Fig. 5, we can easily see that the misdetection ratio of our IDS is lower than WTA. Recall that the multi-dimension characteristic monitor method is adopted in our IDS which will lead more accurate judgment when the network facing with many types attack simultaneously. What's more, as a subjective concept, the running state of the evaluated SN can be reflected more accurately by using evidence theory. Taking these two points, the proposed IDS maintain lower misdetection ratio than WTA.

## CONCLUSION

As a new technology, wireless sensor networks have been extensively studied in recent years, at the same time, the security issue of it has attracted more and more attention. In this study, a novel IDS based on evidence theory for CWSN is introduced. Each CH collects the behaviors of its cluster member node from four aspects and then constructs the input evidence according to the deviation from normal level. Before evidence synthesis, weight mechanism is used to revise the BPA value according to behavior's history contribution. Finally, combined with evidence theory and judgment rules, the running state of the evaluated SN is obtained. The simulation results show that our IDS achieves high detection ratio and low misdetection ratio at the same time. In the next study, we will try to integrate our IDS with routing algorithm or data fusion algorithm which will further enhance the reliability of WSNs.

## REFERENCES

Akyildiz, I.F., W. Su, Y. Sankarasubramaniam and E. Cayirci, 2002. Wireless sensor networks: A survey. Comput. Networks, 38: 393-422.

Alemdar, A. and M. Ibnkahla, 2007. Wireless sensor networks: Applications and challenges. Proceedings of the 9th International Symposium on Signal Processing and Its Applications, February 12-15, 2007, Sharjah, UAE., pp: 1-6.

Chang, Y. and F. Liu, 2011. Wireless sensor intrusion detection system based on the theory of evidence. Proceedings of the International Conference on Computer Science and Network Technology, Volume 4, December 24-26, 2011, Harbin, China, pp: 2811-2814.

Chen, L., W. Shi and F. Du, 2005. New weighting factors assignment of evidence theory based one vidence distance. J. Syst. Eng. Electron., 16: 273-278.

Dempster, A.P., 1967. Upper and lower probabilities induced by a multivalued mapping. Ann. Math. Stat., 38: 325-339.

Depren, O., M. Topallar, E. Anarim and M.K. Ciliz, 2005. An intelligent Intrusion Detection System (IDS) for anomaly and misuse detection in computer networks. Expert Syst. Appl., 29: 713-722.

Haddadi, F. and M.A. Sarram, 2010. Wireless intrusion detection system using a lightweight agent. Proceedings of the 2nd International Conference on Computer and Network Technology, April 23-25, 2010, Bangkok, Thailand, pp: 84-87.

Hu, Y.C., A. Perrig and D.B. Johnson, 2003. Packet leashes: A defense against wormhole attacks in wireless networks. Proceeding of the INFOCOM, 22nd Annual Joint Conference IEEE Computer and Communication Society, Mar. 30-Apr. 3, IEEE Publication, pp: 1976-1986.

Ju, L., H. Li, Y. Liu, W. Xue, K. Li and Z. Chi, 2010. An improved intrusion detection scheme based on weighted trust evaluation for wireless sensor networks. Proceedings of the 5th International Conference on Ubiquitous Information Technologies and Applications, December 16-18, 2010, Sanya, China, pp: 1-6.

Lu, G. and W. Xue, 2010. Adaptive weighted fusion algorithm for monitoring system of forest fire based on wireless sensor networks. Proceedings of the 2nd International Conference on Computer Modeling and Simulation, Volume 4, January 22-24, 2010, Sanya, Hainan, China, pp: 414-417.

Moon, S.Y. and T.H. Cho, 2009. Intrusion detection scheme against sinkhole attacks in directed diffusion based sensor networks. Int. J. Comput. Sci. Network Secur., 9: 118-122.

Ribeiro, W., T.H. Palua and P. Junior, 2004. Malicious node detection in wireless sensor networks. Proceedings of the 18th International Parallel and Distributed Processing Symposium, April 26-30, 2004, Santa Fe, New Mexico, USA.

Shafer, G., 1976. A Mathematical Theory of Evidence. Princeton University Press, USA.

Tumrongwittayapak, C. and R. Varakulsiripunth, 2009. Detecting sinkhole attack and selective forwarding attack in wireless sensor networks. Proceedings of the 7th International Conference on Information, Communications and Signal Processing, December 8-10, 2009, Macau, China, pp: 1-5.

Yang, S., X. Wang and L. Fu, 2012. On the topology of wireless sensor networks. Proceedings of the IEEE INFOCOM, March 25-30, 2012, Orlando, FL., USA., pp: 2095-2103.

Zhang, G.Y. and W. Lee, 2000. Intrusion detection in wireless ad-hoc networks. Proceedings of the 6th International Conference on Mobile Computing and Networking, August 6-11, 2000, Boston, MA., USA., pp: 275-283.

Zhou, Y., Y. Fang and Y. Zhang, 2008. Security wireless sensor networks: A survey. Commun. Surv. Tutorials, 10: 6-28.