A Proposal of Cooperative Malicious Behavior Node Isolation Mechanism for Wireless Sensor Networks

Ailixier Aikebaier[1,a)] Masahiro Jibiki[1,b)] Yuuichi Teranishi[1,c)] Nozomu Nishinaga[1,d)]

Abstract: In wireless sensor networks, due to fault and malicious behaviors of network entities, the sensor data collected might be not accurate. Therefore, it is crucial to effectively detect and isolate malicious network entities from the network. Some studies have been demonstrated that rating trust and reputation of individual network entities is an effective approach in wireless sensor networks to improve security, support decision-making process and promote collaboration between network entities. However, trust management systems are prone to the attacks from inside of the network. Insider attacks like selective forwarding and bad-mouthing can significantly deteriorate the trust management systems and results inaccurate trust evaluation of network entities. In this work, based on wireless overhearing mechanism we propose a novel approach which can effectively detect and isolate malicious network entities from the wireless sensor networks. Simulation results shows that, compare to other malicious node detection schemes, the proposed CMBNI scheme detects and isolates the malicious nodes from the network with more than 50% faster speed. In addition, even with 20% malicious nodes in the network, CMBNI scheme can successfully derlivery all messages sent by sensor nodes to the sink node.

1. Introduction

Wireless sensor networks (WSNs) gain increasing acceptance in the information world as an effective means to collect environmental information from physical world. As an essential part of the forthcoming Internet of things (IoT) era, WSNs provides basic infrastructure for the information collection phase. Since WSNs operates based on cooperation among individual network entities (nodes), like routing sensing data to the collection point (Sink node). Therefore, the performance of a individual node can effect overall network performance. In fact, a node may provide services with a low performance level, like dropping messages from other nodes or even refuse to being cooperate with other nodes. The reason for this can be either the node's physical ability to perform the task successfully or being malfunctioning due to attacks by adversary. Trust management systems can be a effective means of revealing malfunctioning nodes in distributed environments like WSNs, if it is calculated accurately. However, the accurate calculation of the trust value itself can be difficult due to insider attacks made by malicious nodes in the network. Insider attack is an important security issue in wireless sensor network (WSN) [1] due to traditional security measures, such as authentication and authorization are ineffective to prevent attacks originated from legal members of the network. Due to resource constraints and wireless communication, nodes in wireless sensor networks are prone to many types of attacks. Compromised nodes may drop packets or inject false packets. Misbehaviors of these insiders are hard to detect and prevent since they are legal members of the network.

Most WSNs contain a sink node (base station) that is connected to a power source and usually equip with much powerful computational capabilities than the sensor nodes. Since sink node has a global view of the network and total trust from the other sensor nodes, it is more effective to deal with insider attacks based sink node's observation and its decision.

In order to implement a robust trust management system, a effective way to monitor neighbor nodes behavior is essential requirement. We observe that many existing trust management systems adopting watchdog [6] as their neighbor monitoring mechanism. But most of them did not consider in depth the weakness of watchdog mechanism against insider attacks conducted by malicious nodes in the network. Without isolate these malicious nodes from attacking trust management systems in the network, it is difficult to provide accurate trust evaluation results and can potentially damage the overall network performance.

In this paper, in order to protect trust management systems, we propose a cooperative-based malicious behavior node isolation scheme for wireless sensor networks. Malicious nodes are defined as physically faulty nodes and compromised nodes which can intentionally generate false reports regarding other nodes and try to avoid being easily detected by the trust management systems. The proposed scheme identifies malicious nodes based on cooperative behavior monitoring between neighbor nodes and by reporting back detected malicious node's information directly to the sink node. Based on malicious reports collected by sensor

[1] National Institute of Information and Communications Technology, 4-2-1, Nukui-Kitamachi, Koganei, Tokyo 184–8795, Japan
[a)] alisher@nict.go.jp
[b)] jibiki@nict.go.jp
[c)] teranisi@nict.go.jp
[d)] nisinaga@nict.go.jp

nodes, sink node identifies the malicious nodes in the network and by sending alert messages to the sensor nodes neighboring with the identified malicious node, effectively isolates the malicious nodes from the network. By centralizing the malicious node detection process to sink node, the bad-mouthing attacks are effectively eliminated. Therefore, overall performance of the wireless sensor network is improved.

The rest of the paper is organized as follows. Section II introduces related research works. In section III, we discuss trust management systems in wireless sensor networks. In section IV, the proposed cooperative malicious behavior node isolation scheme is described. Finally, based on simulation results the conclusion is drawn in section V.

2. Related Works

In literature it has become a common perspective that computing trust value of a network entity in general depends on the direct and indirect interactions between entities. Through direct interaction with neighboring network entities, the monitoring network entity observes and collects first hand information regarding performance of neighboring entities. In other hand, indirect interaction provides recommendations to monitoring network entity regarding targeted networks entity's performance from their stand point of view, these second hand information can be extremely helpful to accurately calculate trust value of a network entity. On the other hand, collection of these second hand information from neighboring nodes and evaluation regarding accuracy of these information is difficult. Specially for wireless sensor networks, it is computationally expensive for a sensor node to collect second hand information from other nodes and compute trust value of neighbor nodes. Therefore, in this work we consider more realistic approach which based on first hand information collected by watchdog mechanism.

Selection of proper trust evaluation metrics, like performance of message forwarding capabilities, remaining battery power of other nodes can also effect the accuracy of trust evaluation result. In [4], based on the traditional communication based trust evaluation authors has introduced a new factor call data trust to the communication trust to more accurately compute trust value of network entities. However, for each network entity to check the data packet going through itself could be very expensive from resource point of view, if we assume the data packet in the network is encrypted in order to protect the data from eavesdropped by third parties, it will extremely difficult and expensive to support point-to-point encryption among all network entities. In this work, we only consider the communication performance, more specifically node performance on message forwarding as the trust evaluation metric for each node, other trust evaluation metrics are not considered because it is out of scope of this paper. We assume there is some kind of cryptography-based authentication mechanism between sensor nodes and sink node and sensing data is encrypted by each node before the data is sent to the sink node. We consider there is no pairwise authentication between sensor nodes, only sink node can decrypt the sensing data encrypted and send by sensor nodes in the network.

Bad-mouthing attack is a malicious attack conducted by malicious nodes which intentionally falsely reports that other nodes are misbehaving and it is also an important security issue in WSNs. This attack can greatly damage the accuracy of the trust management system in wireless sensor networks. In [7], authors proposed a malicious node detection scheme call *ExWatchdog*, which protects network entities from bad-mouthing attacks conducted by malicious nodes. They identified that, in order to not being detected by watchdog mechanism, a malicious node can honestly forwards all messages to sink node but drops the confirmation message send by sink node. This malicious activity can results sender node not being able to confirm message delivery to the sink node and results unnecessary resend of the message by sender. Message resend can increase power consumption and reduces the lifespan of a sensor node. Although, due to watchdog mechanism, drop of the confirmation message by malicious node can be detected by other nodes on the message path from sink node to the sender node, but from the sender point of view the malicious node honestly forwards the message so that it can be wrongly evaluated as a trustworthy node by the sender. This conflict opinion of sender and other nodes regarding malicious node in the message path can result partially partitioning of the network and effects overall network performance. Although, the proposed *ExWatchdog* scheme in [7] can identify bad-mouthing (false report) attacks by malicious nodes, but the cost of finding a new path to sink node is high. In addition, no actions are suggested after detection of a malicious node, this can result malicious nodes can still drop messages from other nodes as part of the message delivery path to the sink node.

In comparison with [7], based on cooperation between neighboring nodes to monitor malicious activities, we propose a more effective way to address the same issue. Our proposed scheme not only detects the malicious nodes in the network but also effectively isolates them from the network with less cost.

3. Trust Management Systems

In this section, the trust management system we assume in our study is described.

3.1 Trust computation

In general, trust management systems works in the following stages:

(1) Node behavior monitoring: Based on transactions between neighbor nodes, each sensor node monitors and records neighbor's behavior such as performance on packet forwarding, correctness of provided recommendation information regarding other neighbor nodes, battery life, location of node, etc. By collecting these different factors regarding neighbor nodes behavior, the trust management system on each sensor node tries to accurately evaluate and compute the neighbor node's trustworthiness. Watchdog is a monitoring mechanism which takes advantage of characteristics of the wireless signal and popularly used in behavior monitoring stage in wireless sensor networks. How accurately a node can monitor neighbor node's behavior can seriously effect the trust evaluation stage.

(2) Trust evaluation: There are many researches regarding eval-

uation of trustworthiness of a sensor node. Bayesian, Entropy, Game-theoretic, and Fuzzy approaches [10] are commonly considered by the research community. As sated in [6], the outcome of the trust evaluation by trust management system can be different depends on trust model which used. For example, when a node is observed successfully forwarded packets S times and dropped the packets F times, the beta trust evaluation model [8] will assign trust value T ($0 \leq T \leq 1$) to this node by following formula;

$$T = \frac{S+1}{S+F+2} \tag{1}$$

For the sensor nodes with no previous transaction records, the formula sets the initial trust value T to 0.5.
On the other hand, entropy trust evaluation model [9] uses entropy function $H(p)$, p is the trust value computed based on beta trust evaluation model. The entropy function $H(p) = -p\log_2 p - (1-p)\log_2(1-p)$ is used to determine the trust value T. The trust value $T(-1 \leq T \leq 1)$ is defined by following formula;

$$T = \begin{cases} 1 - H(p), for\ \ 0.5 \leq p \leq 1; \\ H(p) - 1, for\ \ 0 \leq p < 0.5 \end{cases} \tag{2}$$

(3) Malicious behavior detection: Based on trust evaluation result, a sensor node determines its neighboring node's trustworthiness and based on that initiates or stops further collaboration with it. If a neighbor node's trust value drops below a certain predefined threshold α_T, node will stop interacting with this neighbor and depending on trust policy defined by trust management system may recognizes this neighbor node as suspicious and report it to other nodes. Regarding way of sharing the suspicious node's information with other nodes in the network, we will discuss in details in later sections.

3.2 Consecutive failure

As introduced in [6], consecutive failure made by faulty or malicious nodes has to be consider in order to timely response and detect abnormal activities in the network. If we assume same trust threshold value (α_T) is used through out the network, it will most likely will expose to the insider attackers through node compromise and attacks can be launch without being detected by the trust management systems. If we assume trust threshold value of a network $\alpha_T = 0.7$ which means nodes with trust evaluation value less than this number is considered as not trustworthy by other nodes and can be subject to malicious behaving node. In order to not being detected, malicious node can build up its trust value by initially successfully forward certain number of packages, it can drop considerable number of packets consecutively without bringing its trust value to 0.7 or below. For example, with $S = 1000$ previous successful forwarding, the next 428 packets can be dropped without being detected by the beta trust evaluation model, and 170 packets can be dropped if the entropy model is used [6]. Malicious nodes can take advantage of this weakness of trust evaluation procedure and damage the network by dropping packets while staying undetected by trust management system.

3.3 Attacks on trust management systems

Unlike noise and faults, malicious nodes can intentionally generate wrong reports regarding other genuine nodes in order to damage network integrity and accuracy of trust management systems in the network.

As long as trust management system consider recommendations (second hand information) from neighboring nodes as one of the evaluation factors, malicious nodes can provide dishonest recommendations to disturb trust evaluation procedures and results inaccurate trust evaluation of network nodes. This attack is referred as the bad-mouthing attack. Bad-mouthing attack has been recognized and discussed in many trust related research works [11], [12]. The most effective way to eliminate bad-mouthing attack is through cross-checking the correctness of the information provided by a malicious node with other nodes. But in WSNs, due to resource constrain specially power limitation of each individual nodes, it is difficult to frequently exchange messages with other sensor nodes to verify the correctness of a information. More over it is possible the neighboring node which provides verification information itself can be a malicious node. To address bad-mouthing attacks in WSNs, we proposed sink-based centralized approach with less additional computational overhead to each sensor nodes.

3.4 Watchdog mechanism

Watchdog is a kind of behavior monitoring mechanism based on characteristics of wireless communication, and it is the most important part of many trust management systems in WSNs. As shown in the Figure 1, we assume the sender node S would like to deliver a message to node R, but due to insufficient signal range of node S, node S is not able to directly communicate with node R. Therefore, node S requires one of its neighbor nodes A which is connected with node R to forward the message to node R. By taking advantage of the characteristics of wireless signal, when node A forwards the message to node R, the sender node S can also detects the transaction and be able to know weather or not the message is forwarded. This is the basic idea of watchdog mechanism, by overhearing wireless signal generated by neighbor nodes, the sender node can monitor the behavior of the neighbor nodes. If node A honestly forwards the message required by node S to node R, then node S positively evaluates the behavior of node A as a reliable candidate for message forwarding, based on these observations the trust management system on node S computes node A's trust value. The trust value of neighbor nodes are used to assist decision making process of sensor nodes, like routing and malicious node detection, etc.

Although the watchdog mechanism seems to be a very effective way to monitor behavior of neighbor nodes, but in some cases, it fail to detect the malicious activities of neighboring nodes. As shown in Figure 2, we assume the sender node S would like to deliver a message $Sig_s(Mes_s)$ to receiver node R through relying nodes A and X. If we suppose that, the node X is a malicious node and drops only confirmation messages send by receiver node R. Then, for node A by using watchdog mechanism it can only detect node X is forwarded message to node R, but will not able to detect

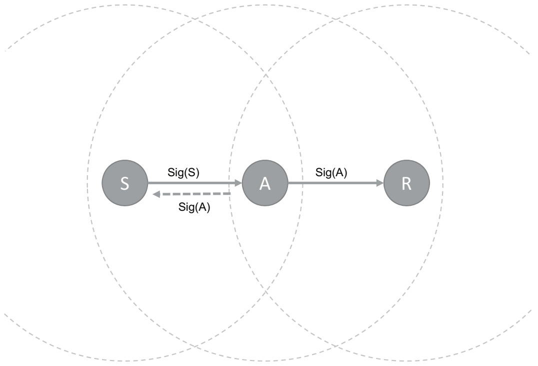

Fig. 1 Watchdog mechanism

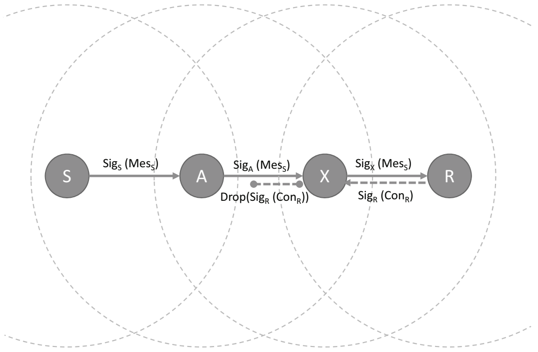

Fig. 2 Drop Ack attack.

dropped confirmation message by node X. Here, even node X is a malicious node and dropping the confirmation messages from receiver node R, the node A still evaluate it as a trustworthy node because of the forwarding performance of node X. On the other hand, the receiver node R can detect that node X is dropping confirmation messages which it sends and decreases the trust value of node X. This can results an conflict trust evaluation regarding node X in the network. For node A, the malicious node X can maintain high trust value even while dropping confirmation messages from receiver node R.

The serious weakness of watchdog mechanism is that, because the malicious node can maintain its trust value relatively high on some of its neighbor nodes by selectively dropping the messages, like node A in the previous example, it can falsely report other nodes as misbehaving. Because of incorrect high trust value of malicious node, the other nodes might trust its false report regarding other nodes and incorrectly marks honest sensor nodes as untrustworthy or even malicious. Therefore, a malicious node could partition the network by falsely accusing other genuine neighboring nodes as misbehaving.

Thus, as long as there are malicious nodes in the network, it is difficult to evaluate other nodes behavior even based on reports from trustworthy neighboring nodes. To avoid bad-mouthing (false report) attacks conducted by malicious nodes, we take advantage of the characteristics of the WSNs, which is all sensor nodes deliver it is sensing data to sink node and sink node is the one of the most trustworthy node in the network. We proposed a sink-based approach which is instate of trusting reports from other nodes, every sensor nodes only trusts reports send by sink node. If any sensor node detects misbehavior of its neighboring node, it reports the suspected node's information directly to the sink node. We present a detailed description of the proposed scheme in the following section.

4. Cooperative Malicious Behavior Node Isolation (CMBNI) Scheme

Based on watchdog mechanism in wireless networks, we propose a cooperation-based malicious node detection and isolation scheme. The proposed cooperative malicious behavior node isolation (CMBNI) scheme can effectively detect and report malicious behavior of nodes to sink node and based on centralized decision made by sink node effectively isolates malicious behavior nodes from the network. The advantage of the proposed scheme is that, the identification of malicious nodes are performed by sink node only according to the reports collected by sensor nodes, this can effectively eliminate bad-mouthing attacks from malicious nodes. In addition, the proposed algorithm can achieve its objectives with less overhead to the sensor nodes, because most of the computational parts of the scheme are executed on sink node which usually has more power and other resources comparing to the sensor nodes.

4.1 Cooperative-based behavior monitoring

The basic idea is that, instead of only monitoring messages send by itself through watchdog mechanism, the sensor node also monitors the transaction activities between neighbor nodes. If node detects malicious activities of neighbor nodes like message drops, it reports information of suspected malicious node to sink node. Therefore, for each transaction between two sensor nodes, not only the sender monitors the behavior of the rely node but also other neighbor nodes will cooperatively monitor the transaction. If relay node drops the message, sender node and other cooperative neighbor nodes can detects the misbehavior of the node and simultaneously reports the suspected node to the sink node. After receiving the multiple reports regarding a malicious node from different sensor nodes, sink node can easily identify the malicious node and take further actions.

For example, as shown in the Figure 3, we assume node S sends a message $Sig(S)$ to node R through rely node A. Node M is a common neighbor of node S and A since it can receive wireless signal from both nodes. Since common neighbor node M can overhear the message $Sig(S)$ send by node S to node A and also can monitors the wireless signal generated by node A, it will in cooperate with node S simultaneously monitor the behavior of node A. If node A drops the message send by S, not only sender node S but also cooperative node M can detect misbehavior of node A and reports back node A as a suspicious node to the sink node. Based on reports received from node S and M sink node identifies node A as a malicious node.

The major benefit from cooperative-based behavior monitoring mechanism is that, the sink node identifies the malicious nodes based on multiple reports from sensor nodes. Compare to a single report, the sink node can more reliably identifies the malicious node and eliminates the bad-mouthing (false report) attacks, because usually the bad-mouthing attack is conducted by a single malicious node. The sink node make its decision based on multiple reports regarding to a single suspicious node. In other words, the sink node will ignore if the report is made by a single node and there are no other nodes are reporting the same node as suspicious.

For practical WSNs applications, it is the common case that in order to provide node connectivity and redundancy of message delivery, sensor nodes are densely deployed in the network. Thus, it is more likely to find common neighbor nodes like M in the network as shown in Figure 3 and perform cooperative malicious behavior detection scheme.

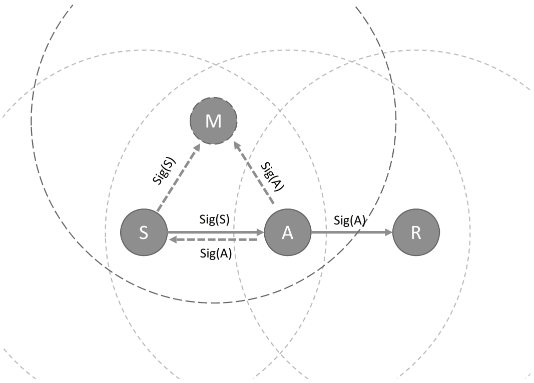

Fig. 3 Cooperative watchdog

4.2 System description

Each node in the network is equipped with a watchdog module which not only monitors the messages send by itself but also monitors the transactions between its neighbor nodes. If one of the monitored neighbor node consecutively drops the messages for several times, the monitoring node identifies it as a suspicious node and reports back to the sink node. Because each transaction between two sensor node is cooperatively monitored by multiple nodes, the misbehavior of a malicious node can be simultaneously detected by multiple sensor nodes. If sink node receives multiple reports regarding misbehaving of a individual node, it quickly identifies the misbehaving node as a malicious node and sends an alert message to neighbor nodes of that malicious node. After receiving the alert message from sink node, the neighbor nodes of the malicious node isolates it from its neighbor list. Since the alert message is signed by the sink node, for each sensor nodes there is no need to verify the trustworthiness of the message because the sink node is the most trustworthy node in the network. For a detected malicious node in the network, sink node not only confirms the sensor nodes who reported the suspicious node by alert message, but also informs the other neighbor nodes of the detected malicious node which has not yet recognizes the malicious node. This prorogation of malicious node information by sink node can effectively isolate the malicious node from all its neighboring nodes, reduces the further damage results by the malicious node to the network.

5. Simulation

Computer simulation is conducted to evaluate the effectiveness of our proposed cooperation-based malicious behavior node isolation (CMBNI) scheme.

Based on same simulation settings, proposed CMBNI scheme is compared with trust evaluation scheme which has no continuous failure detection mechanism denoted as T_NCFD and trust evaluation scheme with continuous failure detection mechanism denoted as T_CFD. The proposed scheme is denoted as CMBNI during the simulation. Although both CMBNI and T_CFD schemes can detect consecutive failures by malicious neighbor nodes and compute trust value of neighbors based on this observation, but the main difference between T_CFD and CMBNI is after detecting a malicious activity of a neighbor node weather or not it reports back this information to the sink node. Performance of the T_NCFD, T_CFD, and CMBNI schemes are compared in the network set with different malicious node ratios.

5.1 Simulation setups

To avoid random factors from simulations, grid structured network is selected for the simulation environment. Same transmission range r is chosen for each sensor node to set their number of neighbor nodes at maximal equal to 8 to minimal equal to 3 (nodes at the corner of the grid network). Based on following two different scenario settings, we compared the performance of the proposed scheme with others.

(1) Sink node in the center of the network.
(2) Sink node at the corner of the network.

For scenario (1), which sink node is positioned in the center of the grid network, 80 sensor nodes are deployed. Based on malicious node ratio (10% ~ 40%) of the network, randomly and manually generated malicious nodes are positioned in the netowrk. As malicious node behavior, only the confirmation messages through the malicious node are dropped. For the general nodes, each node tries to deliver sensing data to sink node in form of a message. After sending the message to the sink node, each node waits for confirmation message from sink node. With in timeout period t_{out}, if confirmation message is received from sink node, the transaction is counted as a successful message delivery. In other hand, if no confirmation message received from sink node within the time out period, the sender node resends the same message to sink node again. The sender node repeats this action until receives confirmation message from the sink node. For scenario (2), except sink node 99 sensor nodes are deployed in grid network. Other settings are same as for the scenario (1).

Three metrics, message delivery ratio (MDR), total message drop (TMD), and total resend messages (TRM), are defined to evaluate the proposed scheme and others. MDR is defined to be the ratio between the number of sensor node which successfully delivered a message to sink node and the total sensor node which sends a message to sink node. A successful message delivery by a sensor node is measured by message send by the sensor node and corresponding confirmation message received from the sink node. After sending a message to sink node, if corresponding confirmation message is not receive, sensor node resends the same message to sink node again and waiting for a confirmation from sink node. Message with no confirmation is not counted as successful message delivery. Illegal message drop by malicious nodes can be the main reason for sensor nodes being not able to confirm message delivery to the sink node. High MDR means even with present of malicious nodes in the network, sensor nodes can successfully delivery its sensing data to sink node.

5.2 Simulation results

From simulation results we can identify that, the proposed scheme (CMBNI) performed batter compare to the other schemes. Figure 4 and figure 5 shows message delivery ratios with different malicious node ratio settings in case of sink node in the center and edge of the network, respectively. As expected, for both scenarios (center, edge), similar simulation results are collected, which shows the proposed scheme is performed better compare to the others. Even in the case of 20% malicious nodes in the network, the propsed CMBNI scheme maintained successful message delivery ratio close to 100% .

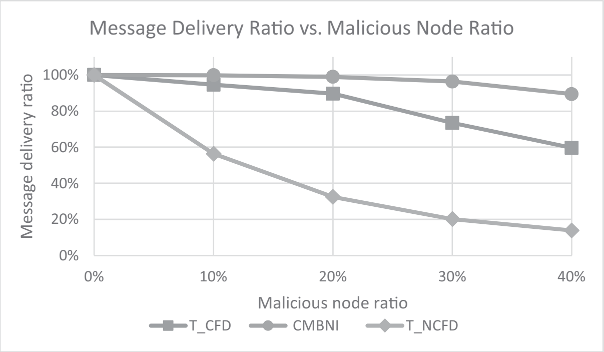

Fig. 4 Message delivery ratio vs. Malicious node ratio (Sink center).

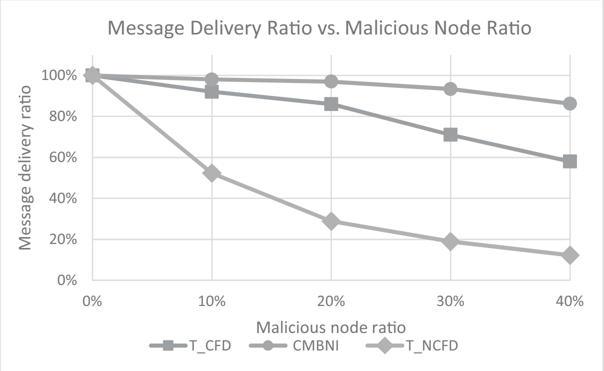

Fig. 5 Message delivery ratio vs. Malicious node ratio (Sink edge).

From Figure 6 and 7, we can also conclude that because of the fast detection and isolation of malicious nodes from the network, less messages are dropped by malicious nodes in the network. The proposed scheme successfully eliminated the damage resulted by malicious nodes to the network.

Figure 8 and 9 also shows that, because of the effective malicious behavior node isolation of the proposed scheme, less number of messages are being resend compare to the other schemes.

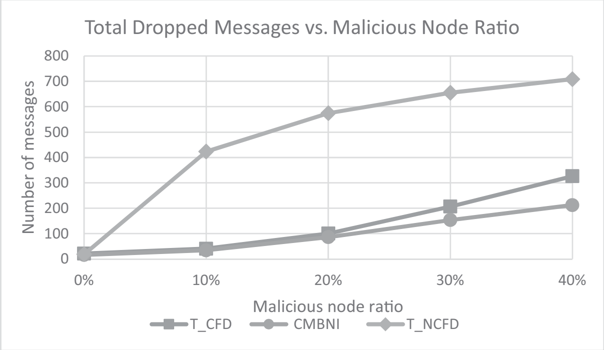

Fig. 6 Total message drop vs. Malicious node ratio (Sink center).

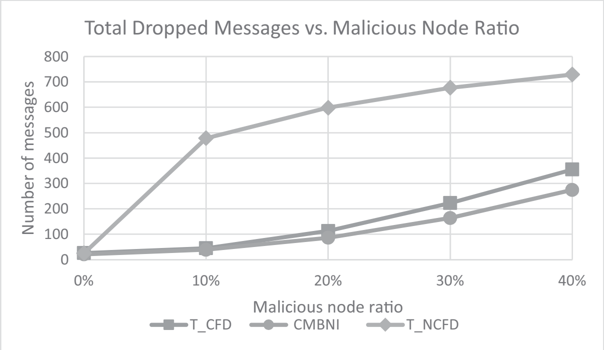

Fig. 7 Total message drop vs. Malicious node ratio (Sink edge).

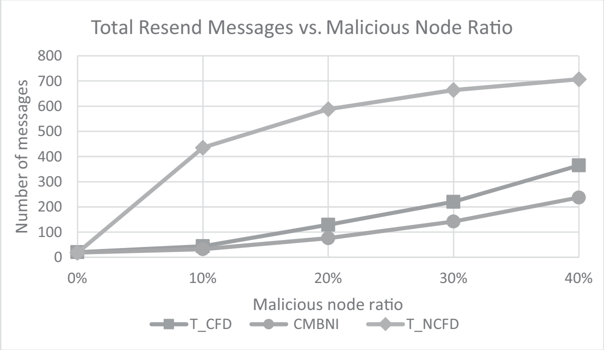

Fig. 8 Total resend message vs. Malicious node ratio (Sink center).

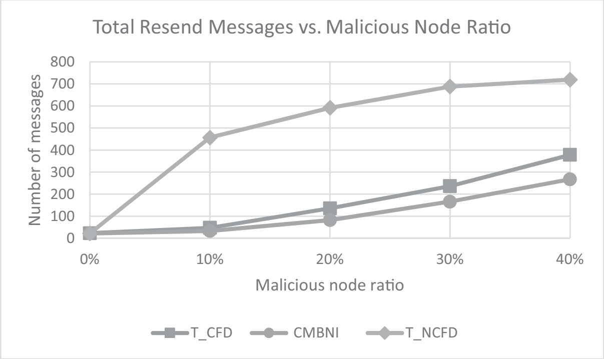

Fig. 9 Total resend message vs. Malicious node ratio (Sink edge).

In Figure 10, more specific performance comparison between proposed scheme CMBNI which reports malicious detection results to the sink node and T_CFD scheme which avoids the detected malicious nodes in the future interactions are presented.

The metrics EXT measures the average time which takes all sensor nodes in the network to successfully deliver a message to sink node. In order to successfully deliver a message to sink node, for each node a path with no malicious nodes present has to be discover. Thus, EXT shows how fast the sensor nodes can detect and exclude the malicious nodes from the messages delivery paths. The simulation results shows that, the proposed scheme greatly outperformed the T_CFD scheme which simply avoid the detected malicious nodes. Other metrics like DM which stands for the dropped messages by malicious nodes and RM which stands for the resend messages by sensor nodes also indicates that because of the effectiveness regarding isolation of malicious nodes from the network, the proposed algorithm can also greatly reduce the damage resulted by the malicious nodes. Metrics NN, SM, and CM stands for number of nodes in the network, number of messages send by sensor nodes, and number of confirmed message delivery by sensor nodes, respectively. Because of the same simulation setting, NN, SM, and CM shows same value for T_CFD and CMBNI schemes. Metric TM stands for total messages send by sensor nodes, which shows the proposed CMBNI scheme generates less number of messages during the simulation compare to T_CFD scheme. For WSNs, less number of messages means less power consumption for each sensor nodes.

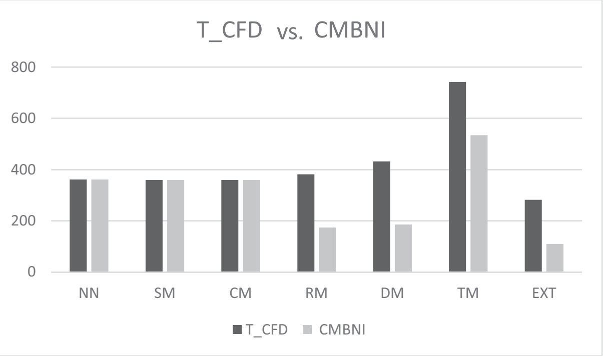

Fig. 10 T_CFD scheme vs. CMBNI scheme

6. Conclusion

Security is one of the most important aspects has to be concern in wireless sensor networks (WSNs) before deployment and practical use in the real-world scenarios. Because of the characteristics of the WSNs, it is difficult to directly apply traditional security measures on it. Trust management systems has recently been recognized as one of the most effective ways to improve the overall security of WSNs, specially for insider attacks by malicious network entities. To build a robust trust management system in WSNs, the malicious attacks which targets trust management systems has to be concern. Without eliminating these attacks, it is difficult for a trust management system to provide trustworthy node evaluation information to the network. Based on watchdog mechanism in WSNs, we proposed a cooperative-based malicious behavior node isolation scheme. Simulation results shows that, the proposed CMBNI scheme can effectively detects and isolates malicious nodes from the network. Even with 20% of malicious nodes in the network CMBNI scheme ahieved message delivery ration close to 100%. Effective isolation of malicious behaving nodes not only protects the trust management system itself but also results on performance gain due to less number of messages dropped by malicious nodes. Compare to other malicious node detection schemes, the proposed CMBNI scheme detects and isolates the malicious nodes from the network with more than 50% faster speed.

References

[1] Akyildiz, I.F., Weilian Su, Sankarasubramaniam, Y., Cayirci, E.: A survey on sensor networks, *IEEE Communications Magazine*, Vol. 40, No. 8, pp. 102–114 (2002).

[2] Boukerch, A., Xu, L., EL-Khatib, K.: Trust-based Security for Wireless Ad Hoc and Sensor Networks, *Computer Communications*, Vol. 30, No. 11-12, pp. 2413–2427 (2007).

[3] Papaioannou, T.G., Stamoulis, G.D.: Effective use of reputation in peer-to-peer environments, *In: Proceedings of IEEE/ACM CCGRID 2004, GP2PC Workshop*, pp. 259–268 (2004).

[4] Momani, M., Challa, S., Alhmouz, R.: Can we trust trusted nodes in wireless sensor networks?, *In: International Conference on Computer and Communication Engineering (ICCCE 2008)*, pp. 1227–1232 (2008).

[5] Sun, Y., Han, Z., Yu, Liu, K.J.R.: Attacks on Trust Evaluation in Distributed Networks, *Proc. 40th Annual Conference on Information Sciences and Systems (CISS)* pp. 1461–1466 (2006).

[6] Youngho Cho, Gang Qu, Yuanming Wu: Insider Threats against Trust Mechanism with Watchdog and Defending Approaches in Wireless Sensor Networks, *In: IEEE Symposium on Security and Privacy Workshops (SPW 2012)*, pp. 134–141 (2012).

[7] Nasser, N., Yunfeng Chen: Enhanced Intrusion Detection System for Discovering Malicious Nodes in Mobile Ad Hoc Networks, *In: IEEE International Conference on Communications (ICC '07)* pp. 1154–1159 (2007)

[8] Josang, A., Ismail, R.: The Beta Reputation System, *In: 15th Bled Electronic Commerce Conference* (2002).

[9] Sun, Y.L., Han, Z., Liu, K.J.R.: Defense of trust management vulnerabilities in distributed networks, *IEEE Communications Magazine*, Vol. 46, No. 2, pp.112–119 (2008).

[10] Yanli Yu, Keqiu Li, Wanlei Zhou, Ping Li: Trust mechanisms in wireless sensor networks: Attack analysis and countermeasures, *In: Journal of Network and Computer Applications, Elsevier*, Vol. 35, No. 3, pp. 867–880 (2012).

[11] S. D. Kamvar, M. T. Schlosser, H. Garcia-Molina: The eigentrust algorithm for reputation management in p2p networks, *In: 12th International World Wide Web Conference*, (2003).

[12] C. Dellarocas, Mechanisms for coping with unfair ratings and discriminatory behavior in online reputation systems, *In: 21th International Conference on Information Systems (ICIS)*, pp. 520–525 (2000)