Graduate Research in Engineering and Technology (GRET)

Volume 1 | Issue 1 Article 9

July 2013

FALSE MISBEHAVIOUR ELIMINATION IN WATCHDOG MONITORING SYSTEM USING CHANGE POINT IN A WIRELESS SENSOR NETWORK

A. BABU KARUPPIAH
Velammal College of Engineering and Technology, Madurai, India, a_babukaruppiah@gmail.com

FALSE MISBEHAVIOUR ELIMINATION IN WATCHDOG MONITORING SYSTEM USING CHANGE POINT IN A WIRELESS SENSOR NETWORK

A.BABU KARUPPIAH[1], T.MEENAKSHI[2], T.I.MANO RANJITHA[3] & S.VIVITHA[4]

[1]Assistant Professor, [2,3,4]Final Year Students, Velammal College of Engineering and Technology, Madurai, India

Abstract- Wireless Sensor Networks are to be widely deployed in the near future for data monitoring in commercial, industrial and military applications. Though much research has focused on making these networks feasible and useful security has received very little attention. Sensor networks are exposed to variety of attacks like eavesdropping, message tampering, selective forward, gray hole attack, and Wormhole and Sybil attacks. Watchdog is a kind of behaviour monitoring mechanism which is the base of many trust systems in Ad hoc and Wireless Sensor Network. Current watchdog mechanism only evaluates its next-hop's behaviour and propagates the evaluation result to other nodes by broadcasting, which is neither energy efficient nor attack resilient. The fundamental problem of secure neighbour discovery is studied which is importunate in protecting the network from different forms of attacks. In this paper an improved watchdog monitoring mechanism is proposed by using the process of change point detection. By implementing this change point detection algorithm in watchdog mechanism, the limitations of the existing watchdog mechanism are overcome. From this the exact malicious node can be found out and the data will be routed through a secure path bypassing the malicious node. Finally to analyze the efficiency of this algorithm, the results obtained from the proposed algorithm and the existing algorithms are compared.

I. INTRODUCTION

Wireless Sensor Networks have been used in every type of environment due to their easy deployment. WSNs provide their users with fast and easy access to their data and services even in remote areas such as battlefield, forest and volcano. In these security sensitive deployments, keeping the network available for its intended use is essential. But communications over wireless channels are, by nature, insecure and easily susceptible to various kinds of threats. An adversary can control a sensor node undetectably by physically compromising the node and use the captured nodes to inject faulty or false data into the Network system disturbing the normal cooperation among nodes. Authentication and Cryptographic mechanisms alone cannot be used to solve this problem because internal adversarial nodes will have valid cryptographic keys to access the other nodes of the networks. Insider threat is also an important security issue in wireless sensor networks because traditional security mechanisms cannot catch insider attackers as they are legal members of the network. These attackers can disrupt the network by dropping, modifying or misrouting the data packets. This is a very serious threat for many applications such as military surveillance system that monitors the battlefield and several other infrastructures.

II. WATCHDOG MECHANISM

Watchdog is a monitoring mechanism introduced to identify the misbehaving nodes in the network [1][6]. In this approach each sensor node has its own watchdog that monitors and records its one hop neighbours behaviour such as packet transmission. When sending node A sends a packet to its next node B, the watchdog in A verifies whether B forwards the packet to the next node or not by using its overhearing ability within its transceiver range But watchdog has the limitation [2] of not being able to detect the misbehaving nodes in the following conditions.

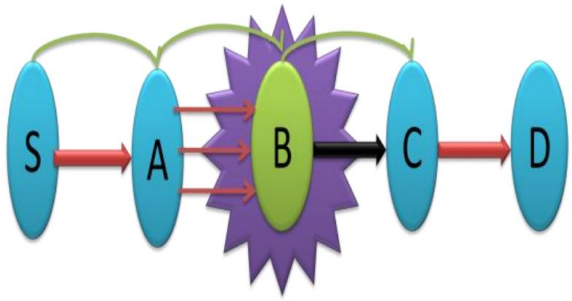

Fig 1 Existing Watchdog Mechanism

1) Ambiguous collision: Consider A forwards a packet to B and overhears whether b is forwarding it or not. When B forwards it to C, A may not overhear this transmission if other neighbours of A send packets to it at the same time. This may mislead A to conclude that B is malicious but this may not be correct.

2) Receiver collision: Collision may occur at the receiver side also (i.e.) C may not receive the packet. A can overhear that B has forwarded the packet, but it cannot tell whether C has received the packet.

3) Limited transmission power: If B can adjust its

transmission power such that A can overhear but C does not receive, then B can drop packets and prove its trustworthiness.

4) False misbehavior: A malicious node intentionally reports that other nodes are misbehaving. A can report that B is dropping packets although B is not. In this case A's neighbor node S which cannot communicate directly with B, can consider B as malicious.

5) Partial dropping: Instead of dropping all packets, B can drop only some packets such that the failure tally will not exceed the detection threshold of A's watchdog.

III. RELATED WORK

A mechanism based on signal strength [5] was proposed to detect the malicious nodes in a network. The idea was to compare the signal strength of a reception with its expected value. A signal is only detected by a receiving node if the received signal power is equal or greater than the received signal power threshold. If the signal power received is less than the threshold then the particular node is suspected to be malicious.

This may not be true for all cases. A signal power can be weakened due to various reasons like environmental factors, weak signal strength etc. In this case the probability of detecting or suspecting a regular node as malicious node is high.

Hence the reliability of the system is not satisfactory.

To overcome the above said limitations watchdog monitoring system was improved by adding a threshold mechanism [4][12]. In this mechanism, S stores all recently sent packets in its buffer, and compares each packet with the overheard packet to see whether there is a match. If yes, it means that the packet is forwarded by T and S will remove the packet from the buffer. If a packet remains in the buffer for a period longer than a pre-determined time, the watchdog considers that T fails to forward the packet and will increase its failure tally for T. If a neighbours' failure tally exceeds a certain threshold, it will be considered as a misbehaving node by S.

IV. PROPOSED WORK

The objective is to improve the existing watchdog monitoring system by implementing the change point detection algorithm [3] in it, thereby detecting the exact malicious node in the network.

This algorithm will be able to detect the malicious nodes after some attacks have occurred in the process of data collection.

Algorithm 1: Change Point Detection

Input:

A WSN with a collection of sensor nodes S= $\{S_0,S_1, \ldots, S_n\}$, a source node S_0, a sink node S_k and a collection of malicious nodes $S_m=\{S_i, S_{i+1}, \ldots, S_j\}$, where $S_0,S_k \in S$

Output:

S_0 sends a series of data packets = $\{D_1, D_2, \ldots, D_m\}$ to S_n with a time interval of Δt D

for each intermediate node S_{mi} on a routing path from S_0 to S_k

end loop

S_k verifies their sequential numbers

if S_k detects a discontinuous sequential number

S_k broadcasts an alert packet

end if

for each intermediate node S_{mi} receiving the alert

S_{mi} verifies the packets within its cache

if S_{mi} detects a missing packet

S_{mi} sends back an alert to S_k

else

S_{mi} sends back a normal response packet

end if

end loop

if S_k receives a collection of response packet

if an intermediate node S_{mi} does not send back a response

S_k records the identity of S_{mi}

end if

S_k analyzes the status information of the nodes on the routing path

S_k finds out the malicious nodes

S_k broadcasts the identity of malicious nodes

end if

end loop

Here the sink receives a collection of response packets from the nodes in the routing path and analyses these packets to detect the malicious nodes. The status of a node is represented by a status bit. We consider that a node replies 1 for a negative packet and 0 for a positive packet. The node which does not send a reply is considered as -1.So the sink receives all the response packets and creates a list of status bits for the nodes in the routing path. The

status for each round of response can be denoted by a status vector bi=[b1,b2,...bn] ∀ bi ∈ {-1,0,1}. From the status vector the sink groups all the nodes with status bits value of -1 into a separate set Sw. This set contains the collection of nodes which do not respond to the sink. The nodes in Sw are considered as suspicious nodes rather than malicious nodes because some of the nodes in the routing path may fail to receive or send packets due to interference or low communication quality. Hence Sw is called as suspicious set. The sink pays more attention to these nodes in subsequent data collection. To any, if bi-0=0 or -1 and bi=1, then bi-1 is a change point in B. The sensor node on the routing path where the value of status bit changes from 0 or -1 to 1 is referred as the change point. The node identified as the change point along with its immediate upstream and downstream nodes form the malicious sequence. The neighbour nodes of the malicious nodes become the threatened nodes. Distinguishing the malicious and threatened nodes is not necessary because the threatened nodes are not secure for routing. Hence both nodes should be excluded from the routing path. In case of more than one malicious node in a routing path the above said analysis is performed several times to obtain a malicious set. Our proposed algorithm involves the implementation of this change point algorithm in the existing watchdog mechanism.

Algorithm 2: Implementation of Change Point Detection Algorithm in Watchdog Mechanism

INPUT:

S_0 – Source node S_i, S_{i+1}……S_n – Input node

S_k – Sink node, S_{mi} - Malicious node

OUTPUT:

For each S_i watches S_{i+1} whether data sent successfully or not

At the same time S_0 sends the data to the S_i

If S_{i+1} is a true node

response bit of S_i is zero

else

response bit of S_i can send zero or one

end if

End loop

When it reaches S_n all the response bit will be send to the S_k

S_k receives two set of response bits

By fixing the change point the exact S_{mi} will be found out.

Here the responses from the watchdog nodes are taken into consideration. By implementing this algorithm, the nodes exhibiting false misbehavior can be exactly identified and excluded from the routing path. The malicious node might be able to change its transmission power and deceive the watchdog. But using our proposed algorithm even such nodes can be rightly identified. An added advantage is that the present threshold mechanism of the watchdog monitoring systems can be eliminated by using this algorithm. All the limitations of watchdog mechanism that have been mentioned above are found to be eliminated using our algorithm. The sink will broadcast the identities of the nodes found to be k malicious. So the other nodes will exclude these nodes from the routing path.

V. EXPERIMENTAL RESULTS & COMPARISON

In the network setup that is considered it is assumed that the source node is always a true node. The following are the simulation results. Fig 1 shows the simulation result for change point algorithm.

Fig1 Simulation result for Change Point Detection Algorithm

The following are the results for existing watchdog mechanism involving the detection of malicious and true node. Fig2 shows the result of watchdog mechanism for a true node. Fig3 displays the result of watchdog mechanism for malicious node.

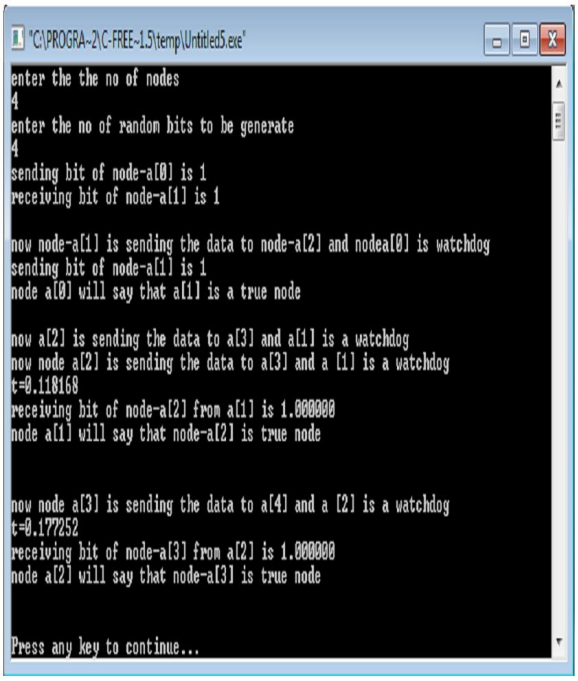

Fig2 Result for Watchdog Mechanism showing true node

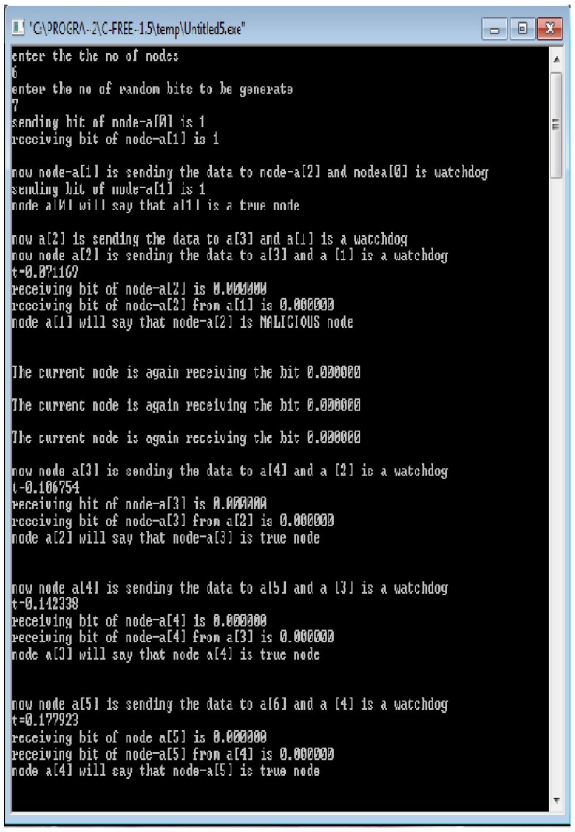

Fig3 Result for Watchdog Mechanism detecting a malicious node

In the case of watchdog mechanism though it declares a node as malicious, it is not completely reliable due to the limitations cited above. On comparing both results, the change point algorithm is found to be more efficient since it is found to detect the exact malicious node under all circumstances.

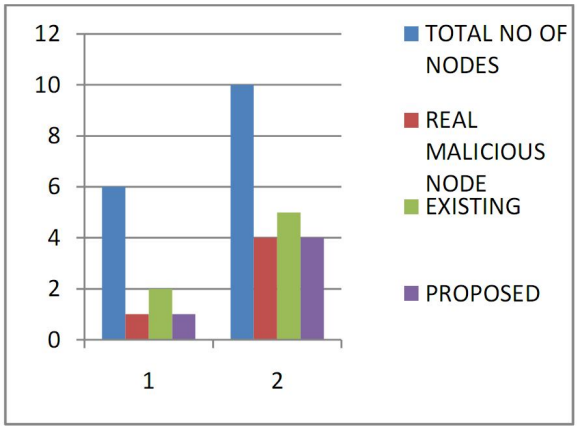

Fig4 Comparison of existing with proposed algorithms.

Fig4 shows the comparison of the existing with the proposed algorithms. The graph is plotted by getting the response bits from each round for both the existing and the proposed algorithms. It shows that the existing algorithm has both the possibilities of detecting the malicious node and also declaring a true node to be malicious. The result of the existing algorithm is not found to be accurate for all the rounds. By using the proposed algorithm the exact malicious node is found to be identified in all the rounds. The malicious node detected by the proposed algorithm is found to be accurate irrespective of the number of rounds conducted.

VI. CONCLUSION

Detection of malicious node is a major concern for security of any network. It is very essential to detect these nodes to prevent the network from loss or tampering of packets. This paper proposes a simple methodology to detect the exact malicious nodes in a Wireless Sensor Network. The future scope of this paper is to remove the exact malicious nodes by implementing this algorithm and to prove that it is also energy efficient when compared with the existing mechanisms.

REFERENCES

[1]. An Improved Watchdog Technique based on Power-Aware Hierarchical Design for IDS in Wireless Sensor Networks A. Forootaninia1 and M. B. Ghaznavi-Ghoushchi, International Journal of Network Security & Its Applications (IJNSA), 2012

[2]. Insider Threats against Trust Mechanism with Watchdog and Defending Approaches in Wireless Sensor Networks Youngho Cho and Gang Qu, IEEE Symposium on Security and Privacy Workshops ,2012

[3]. A Secure Mechanism for Data Collection in Wireless Sensor Networks Yuxin Mao, School of Computer and Information Engineering, Zhejiang Gongshang University, Applied Mathematics & Information Sciences – An International Journal ,2010.

[4]. Extended Watchdog Mechanism for Wireless Sensor Networks Lei Huang +, Lixiang Liu, Journal of Information and Computing Science, 2007

[5]. Malicious Node Detection in Wireless Sensor Networks Waldir Ribeiro Pires J´unior Thiago H. de Paula Figueiredo Hao Chi Wong, 18th International Parallel and Distributed Processing Symposium (IPDPS'04) , 2004

[6]. Reputation and Trust Mathematical Approach for Wireless Sensor Networks Haiguang Chen, Gangfeng Gu , Huafeng Wu, Chuanshan Gao, International Journal of Multimedia and Ubiquitous Engineering,2007

[7]. J. Deng, R. Han and S. Mishra, INSENS: Intrusion-tolerant routing in wireless sensor networks. Computer Communications in Dependable Wireless Sensor Networks, 2006, 29(2), 216-230.

[8]. Y. Wang, G. Attebury and B. Ramamurthy, A survey of security issues in wireless sensor networks. IEEE Commun. Surveys Tutorials, 2006, 8(2), 2-23.

[9]. Y. Zhang and W. Lee, Intrusion detection in wireless ad-hoc networks, Proc. the 6th Annual International Conference on Mobile Computing and Networking, 2000, 275-283.

[10]. S. Sen, et al., "Power-aware intrusion detection in mobile ad hoc networks," Ad hoc networks, pp. 224-239, 2010.

[11]. Y. Wang, "Statistical Techniques for Network Security: Modern Statistically-Based Intrusion Detection and Protection" Idea Group Inc (IGI), 2008.

[12]. Sergio Marti, T.J. Giuli, Kevin Lai, and Mary Baker, “Mitigating Routing Misbehaviour in Mobile and Ad Hoc Networks,” In Proc. Of International Conference on Mobile Computing and Networking (Mobicom), 2000, pp. 255-265

[13]. Chris Karlof and David Wagner, “Secure routing in wireless sensor networks: attacks and countermeasures,” Ad Hoc Networks Journal, Vol.1, Issue 2-3, 2003, pp. 293-315

[14]. Y. Wang, G. Attebury and B. Ramamurthy, A survey of security issues in wireless sensor networks. IEEE Commun. Surveys Tutorials, 2006, 8(2), 2-23.