ISSN No. 0976-5697

Volume 8, No. 5, May – June 2017

International Journal of Advanced Research in Computer Science

RESEARCH PAPER

Available Online at www.ijarcs.info

Channel Aware Detection of Selective Forwarding Attacks in Wireless Sensor Networks

T.C.Swetha Priya
PG Scholar, Department of IT
G. Narayanamma Institute of Technology and Science
JNTUH, Hyderabad, Telangana, India

Dr.I.Ravi Prakash Reddy
Professor, Department of IT
G. Narayanamma Institute of Technology and Science
JNTUH, Hyderabad, Telangana, India

Abstract: Wireless Sensor Networks (WSN) are widely deployed in many applications for their effective event monitoring and data gathering capabilities, so they may be susceptible to Selective Forwarding Attacks in which some of the forwarding packets may be dropped maliciously to reduce the performance of the network. Due to the changing conditions of wireless channel, the packet loss rate may be high and vary with time. **So**, it poses a problem in distinguishing malicious drops from traditional packet loss. This paper proposes an efficient method to detect Selective Forwarding Attacks in Wireless Sensor Networks by penalizing the nodes that are identified to be compromised. To improve detection accuracy, an optimal threshold that is adaptive to the time-varied channel condition is derived. The attack probabilities of malicious compromised nodes is also estimated. The proposed system can identify compromised sensor nodes. It also improves the packet delivery ratio of the network.

Keywords: Malicious node; Selective Forwarding Attack; Packet Delivery Ratio; Data Forwarding Ratio; Reputation System.

I. INTRODUCTION

A Wireless Sensor Network (WSN) has been widely applied to both military and civilian applications for their effective event monitoring and data gathering techniques. Wireless Sensor Networks are applied in unattended and hostile environments. But due to lack of physical protection sensor nodes are easily compromised by malicious nodes making the network vulnerable to selective forwarding attacks. Selective forwarding attack is one of the most severe threats in which the compromised nodes can maliciously drop a subset of packets being forwarded to effect the data delivery ratio and performance of the network. It additionally has considerably negative impacts to information integrity, particularly for data-sensitive applications, e.g., health-care and trade observance. On the other hand, since WSNs are usually deployed in open areas (e.g., aboriginal forests), the unstable wireless channel and medium access collision will cause exceptional traditional packet losses. The Selective Forwarding Attacks are hidden by the conventional packet losses, complicating the attack detection. Therefore, it's difficult to notice the selective forwarding attacks and improve the network performance.

Most of related works target observation of the packet losses in every transmission link and remove the nodes with high packet loss rates from the information forwarding path. These solutions will improve the information delivery or network performance to some extent however they have very little impact on detection of Selective Forwarding Attacks. Since the major challenge in attack detection is to differentiate the malicious drop from normal packet loss, the conventional packet loss rate of the transmission link has to be taken into consideration during forwarding analysis. This tends to take into account the deviation between the conventional losses and actual losses as it is the key issue to detect Selective Forwarding Attacks.

However, for the WSNs deployed in hostile environments wherever the wireless channel is unstable, traditional packet loss rate extremely depends on the wireless channel quality that varies spatially and temporally. If we have a tendency to use a measured or computed traditional packet loss rate to detect selective forwarding attacks, some innocent nodes may be incorrectly judged as attackers owing to the time-varied channel condition. Therefore, a versatile fault tolerant analysis technique is important to accurately identify the attacks and compromised device nodes. Meanwhile, owing to the negative impacts of selective forwarding attacks, Packet delivery ratio of a network becomes the first performance metric for resisting the attacks. Therefore, it is of atmost importance to devise an attack-tolerant routing scheme to use all the nodes or stimulate their cooperation for improving the packet delivery.

In this paper, first a Channel-Aware Trust based System with Adaptive Threshold (CRS-A) [1] based on trust value computation [4] for the detection of Selective Forwarding Attacks in WSNs is proposed. Specifically, we have a tendency to divide the lifetime period of a network into a sequence of evaluation periods. The sensor nodes estimate the conventional packet loss rates between themselves and their neighboring nodes, and adopt the calculable packet loss rates in estimating the forwarding behaviors of its neighbors on the information forwarding path. The sensor nodes misbehaving in forwarding evaluation periods are penalized with reduced trust values. Once the trust value of a node is below a threshold value, it is identified as a compromised node. It also deals with the improvement of packet delivery of a network based on the attack tolerant data forwarding scheme.

II. RELATED WORK

There are basically two main categories of techniques: Acknowledgement based and Neighbor surveillance based schemes according to the packet loss monitoring in each transmission link. The acknowledgement based schemes [8] [10] uses acknowledgements from different nodes in the routing path for finding the packet loss rate of every hop and identify the attacker nodes. If any suspicious behavior is detected it generates alarm packet and deliver to source node. In neighbor surveillance based schemes [3] [5] [7], the sensor nodes monitor their neighboring nodes forwarding behaviors and detect the malicious node misbehavior in the network. But most of the related works have limited capability to accurately detect the attacks and identify the compromised sensor nodes.

These techniques use estimated normal packet loss to evaluate data forwarding behaviors over a long period but such approaches may not be applicable for unstable radio environments. It may cause large false detection probability for innocent nodes. So, the main drawback in the related works is less accuracy in Selective Forwarding Attack detection. In this paper, a CRS-A scheme [1] [2] is proposed to mitigate some of the drawbacks of the existing systems. The main idea of the proposed system is detecting Selective Forwarding Attacks in WSNs and to improve the data delivery ratio of the network.

III. PROPOSED DESIGN

There are two basic modules that are necessary to identify Selective Forwarding Attacks and improve the data delivery ratio of the Wireless Sensor Network. They are: CRS-A [1] and Attack-Tolerant Data Forwarding.

A. CRS-A

In this module, the forwarding behaviors of the sensor nodes are evaluated by using an Adaptive Detection Threshold. Each sensor node maintains a reputation table which includes trust values of each node and their neighboring nodes. These values are used for comprehensive evaluation of forwarding behaviors of nodes. The reputation values are dynamically updated based on the forwarding behaviors evaluated by the neighboring nodes. Reputation Update consists of three procedures: reputation evaluation, propogation and integration. Here the entire network lifetime is partitioned into a sequence of evaluation periods. The reputation (trust value) update is done after each evaluation period.

Initially, the trust value of all the nodes is set to 1.0000. After that based on the received and transmitted packet count, each and every node calculate the trust value of itself and their neighboring nodes also. Then the Threshold value is set to 0.50. If the trust value of a node is below this threshold then the node is suspected to be a malicious node. Then after a certain number of evaluation periods, the reputation values of malicious nodes are significantly reduced in the reputation tables of their neighboring nodes. For the identification of malicious nodes, the nodes send their reputation values to the source after a fixed amount of time. This module is again subdivided into two modules: Packet Loss Estimation and Route Maintenance.

1) Packet Loss Estimation

Due to the unstable wireless channel conditions [9], there may be some noticeable packet losses during wireless transmission, so the normal packet loss should be considered in the evaluation of forwarding behaviors of sensor nodes. So, the Packet Loss is calculated as the difference between the sent and the received packets.

2) Route Maintenance

If there is any route failure, then the intermediate nodes will share the error message to the source node. Based on the error message, the source node will find a new route to destination with Secure Route Discovery model. If a node is identified as malicious, then the route containing that particular malicious node is broken and a new route request is generated by the source node.

Algorithm 1: Cooperation Sensing and Packet Forwarding

1. Initialize the Hello timer
2. If Hello timer expires
   a. Send hello message
3. If node has data
   a. If coop checking not yet over
      i. Get the random neighbor from table
      ii. Send the req to the neighbor node
   b. Else
      i. Send the req to destination
4. If packet received
   a. If the packet is hello packet
      i. If sender is not malicious
         1. If node is unknown node
            a. Add details in table
         2. Else
            a. Update the expire time
      ii. Else
         1. Ignore the packet
   b. If packet is Req packet
      i. Do basic packet filtering and updating operation
      ii. If current node is destination && sender is neighbor
         1. Set packet as Freq
         2. Ignore the packet
      iii. If current node is malicious node
         1. Send reply
      iv. If node is destination
         1. Send reply
   c. If packet is reply packet
      i. If current node is destination of reply packet && source is neighbor
         1. Set packet final node as malicious
         2. Ignore the packet
      ii. Else
         1. Do normal filtering and updating operation

Algorithm 2: Reputation Updation and Data Forwarding in each evaluation period

1. If packet is data type
   a. Data transfer to the shortest path
   b. Initialize Trust=1.0000 for every nodes in a find path
   c. Check for every hop count (Trust = Rx/Tx*100)
   d. Calculated value update to Rtable
      i. If Trust < 0.5 (Threshold)
         1. Update node detail into malicious list
            a. Break link
               i. Generate RREQ to find new route without hacker

ii. Once again data transfer in another route

ii. Else transfer regular data

B. ATTACK TOLERANT DATA FORWARDING

A Collaborative CRS-A [1] Scheme is developed to stimulate the cooperation of compromised nodes and improve the data delivery ratio of the network. To improve the packet delivery ratio of the network, we have to select a better forwarding node using the Data Forwarding Ratio (DFR). The DFR is computed as the ratio of the total number of packets forwarded to the total number of packets sent. In each evaluation period, select the nodes with highest DFR by exchanging the opinion request and opinion reply messages. Each sensor node sends the opinion request about the current route in which data is being sent and based on the opinion reply sent by all the nodes, the path with better forwarding nodes and nodes with high DFR paths will be chosen. This attack tolerant data forwarding scheme will improve the packet delivery ratio of the network.

IV. RESULTS AND DISCUSSION

During simulation, we consider four cases: In the first case, we consider a Selective Forwarding Attack in which some of the packets are maliciously dropped by compromised nodes. The packet delivery ratio in this case is 36%. In the second case, a consequence of the Selective Forwarding Attack is shown in which the compromised node will send a fake routing reply and gets all the packets to be reached to itself instead of destination. In this case, the packet delivery ratio is 0%. In the third case, Cooperation Sensing with Trust based approach is proposed. This helps in identifying the Selective Forwarding Attacks and reduce the packet loss rate. The packet delivery ratio in this case is 63.22%. In the fourth and last case, Cooperation with Trust and Opinion Scores method is proposed to reduce the packet loss and improve the packet delivery ratio of the network to some extent when compared to the first 3 cases. In the last case the packet delivery ratio has increased from 63.22% to 86.45% when compared to the previous case. The Packet Delivery Ratio in all the cases is shown in Fig. 1. The delay is also reduced in the final case when compared to other cases as shown in Fig. 2. The comparison between the four cases mentioned above is shown in Table I.

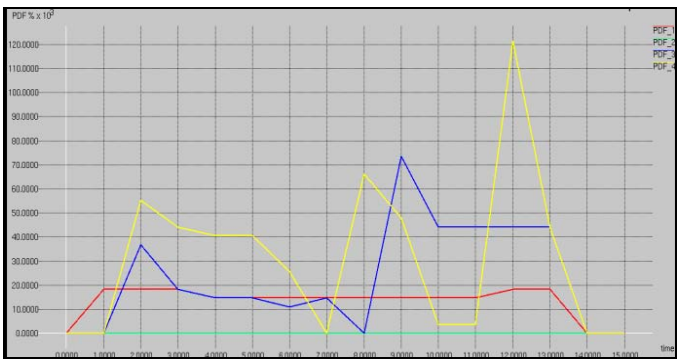

Fig. 1 Packet Delivery Ratio

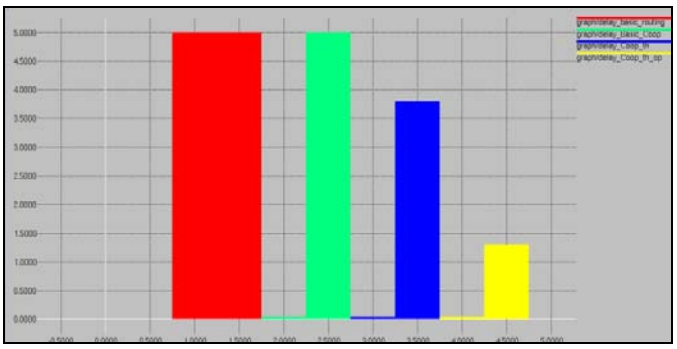

Fig. 2 Packet Delay

Table I. Comparison between the Attack cases, Cooperation with Trust and Cooperation with Trust and Opinion Scores

Parameters	*Cases*			
	Attack 1	*Attack 2*	*Cooperation with Trust*	*Cooperation with Trust and Opinion Scores*
Packets Sent	155	155	155	155
Packets Received	57	0	98	134
Packet Loss	98	155	57	21
Packet Delivery Fraction	36.7741	0.0000	63.2258	86.4516
Average End to End Delay (in seconds)	1.2959	1.9259	0.8619	0.6373

In the above Figures Fig 1 and Fig 2, the red color indicates the case 1 result, the green color indicates the case 2 result, the blue color indicates the case 3 result and the yellow color indicates the case 4 result. From the analysis of these results, we can say that the proposed method is more efficient in improving the packet delivery ratio of the network.

V. CONCLUSION

This paper helps in the detection of Selective Forwarding Attacks in Wireless Sensor Networks by penalizing the nodes that are identified as compromised. An optimal threshold that is adaptive to time-varied channel condition is derived. For the cooperation of compromised nodes in increasing the data delivery ratio of network, an attack tolerant data forwarding scheme is used in collaboration with trust based reputation system [6]. The simulation results show that the projected scheme is able to perform a high detection accuracy with low false and missed detection probabilities. It also identifies the compromised sensor nodes and improves the packet delivery ratio of the network.

VI. FUTURE SCOPE

In the future, the investigation can be extended to WSNs with mobile sensor nodes, where the detection of Selective Forwarding Attacks becomes more challenging, since the normal packet loss rate is more fluctuant and difficult to estimate due to the mobility of sensor nodes.

VII. REFERENCES

[1] J. Ren, Y. Zhang, K. Zhang, and X. Shen, "Exploiting channel-aware reputation system against selective forwarding attacks in WSNs," in Proc. IEEE GLOBECOM, 2014, pp. 330–335.

[2] D. M. Shila, Y. Cheng, and T. Anjali, "Mitigating selective forwarding attacks with a channel-aware approach in WMNs," IEEE Trans. Wireless Commun., vol. 9, no. 5, pp. 1661–1675, May 2010.

[3] B. Xiao, B. Yu, and C. Gao, "CHEMAS: Identify suspect nodes in selective forwarding attacks," J. Parallel Distrib. Comput., vol. 67, no. 11, pp. 1218–1230, 2007.

[4] I. Butun, S. Morgera, and R.Sankar, "A survey of intrusion detection systems in wireless sensor networks," IEEE Commun. Surveys Tuts., vol. 16, no. 1, pp. 266–282, May 2014.

[5] Wazir Zada Khan, Yang Xiang, Mohammed Y Aalsalem," Comprehensive Study of Selective Forwarding Attack in Wireless Sensor Networks", I.J. Computer Network and Information Security, 2011, 1, 1-10.

[6] S. Ozdemir, "Functional reputation based reliable data aggregation and transmission for wireless sensor networks," Comput. Commun., vol. 31, no. 17, pp. 3941–3953, 2008.

[7] X. Li, R. Lu, X. Liang, and X. Shen, "Side channel monitoring: Packet drop attack detection in wireless adhoc networks," in Proc. IEEE Int. Conf. Commun. (ICC), 2011, pp. 1–5.

[8] E. Shakshuki, N. Kang, and T. Sheltami, "EAACK—A secure intrusion detection system for MANETs," IEEE Trans. Ind. Electron., vol. 60, no. 3, pp. 1089–1098, Mar. 2013.

[9] N. Baccour et al., "Radio link quality estimation in wireless sensor networks: A survey," ACM Trans. Sens. Netw., vol. 8, no. 4, pp. 1–34, 2012.

[10] K. Liu, J. Deng, P. Varshney, and K. Balakrishnan, "An acknowledgment based approach for the detection of routing misbehavior in MANETs," IEEE Trans. Mobile Comput., vol. 6, no. 5, pp. 536–550, May 2007.