Adaptive and Channel Aware Forwarding Attack Detection for Mobile Sensor in WSN with Security of Data

Ms. Madhumati V. Kivande
Department of Computer Networking
Smt. Kashibai Navale College of Engineering Vadgaon(BK), Pune & Savitribai Phule Pune University Maharashtra, India

Mr. Adinath M. Wade
Department of Computer Networking
Smt. Kashibai Navale College of Engineering Vadgaon(BK), Pune & Savitribai Phule Pune University Maharashtra, India

Abstract

Wireless Sensor Networks (WSNs) are evolving as a solution for large scale high speed internet access via their self-configuring, scalability and low cost. This project takes a particular kind of DoS attack known as selective forwarding attack that can maliciously drop a subset of forwarding packets to degrade network performance and integrity. Due to the unstable wireless channel in WSNs, the packet loss rate during the communication of sensor nodes may be high and vary from time to time. In this paper, we propose a channel-aware reputation system with adaptive detection threshold (CRS-A) to detect selective forwarding attacks in WSNs. The CRS-A evaluates the data forwarding behaviors of sensor nodes, by monitoring packet loss and the estimated normal loss. To optimize the detection accuracy of CRS-A, using optimal threshold for forwarding evaluation. Furthermore, an attack-tolerant data forwarding scheme is developed to collaborate with CRS-A for stimulating the forwarding cooperation of compromised nodes and improving the data delivery ratio of the network. Contribution in proposed system, providing the authentication of nodes in the multi-hop routing in wireless sensor network. Another one is, showing the less energy power consumption during the detection of malicious node and forward data packet in mobile ad-hoc network.

Keywords: Wireless sensor network, selective forwarding attack, reputation system, packet dropping, channel-aware, multi-hop routing

I. INTRODUCTION

Wireless sensor network (WSN) has been widely used for security monitoring and data gathering technique in both military and civilian applications. Due to the lack of physical protection, sensor nodes are easily compromised by adversaries, making WSN vulnerable to various security threats. The selective forwarding attack, is maliciously dropping packets in the data forwarding network. It also has significantly negative impacts to data integrity, especially for data-sensitive applications. Therefore, it is very challenging to detect the selective forwarding attacks and improve the network performance. In this project, we propose a Channel-aware Reputation System with adaptive detection threshold (CRS-A) to detect selective forwarding attacks in MSNs. As well as detection accuracy follows by two ways: One is, detecting appropriate malicious node in data forwarding path and another one is, normal nodes cannot be falsely detect as malicious node. And data forwarding ratio is improvement. A CRS-A to detect selective forwarding attacks and identify malicious nodes and also attack tolerant routing scheme as follows:

- Reputation Evaluation and Threshold Optimization
- Attack Detection Accuracy
- Data Delivery Ratio

In this paper, we propose detection accuracy of CRS-A technique to detect the selective forwarding attacks by using attack and dynamically updates into the reputation table which shows the malicious node record of the data forwarding path. The data delivery ratio improvement scheme should be able to partly stimulate the co-operation of malicious nodes in data forwarding. Improve the quality of data forwarding path using CRS-A With Attack-tolerant Data Forwarding technique. Minimize the energy power consumption at data forwarding in this WSN of mobile ad-hoc network. CRS-A technique is data forwarding in wireless sensor network securely. This paper has the following enhancements and new contributions.

1) We evaluate the forwarding behaviors of sensor nodes by utilizing an adaptive detection threshold.
2) A distributed and attack-tolerant data forwarding scheme to collaborate with CRS-A for stimulating the forwarding cooperation of compromised nodes and improving the data delivery ratio of the network.
3) CRS-A with attack-tolerant data forwarding scheme can achieve a high detection accuracy with both of false and missed detection probabilities close to 0, and improve more than 10% data delivery ratio for the network.
4) Less the energy power consumption at data forwarding in this WSN of mobile ad-hoc network.

The remainder of this paper is organized as follows. Section 2 Review of Literature. Section 3 introduces the System Architecture. Section 4 describes the Mathematical Model for Proposed work. and Section 5 gives Reputation Score Calculation,

All rights reserved by *www.ijste.org*

Section 6 gives conclusion and advantages of the paper and finally Section 7 gives Future Scope, Section 8 gives Acknowledgement, Section 9 gives References.

II. REVIEW OF LITERATURE

The existing system [1], works into two categories: acknowledgment based and neighbor-surveillance based schemes, according to different monitoring techniques for data forwarding. In a acknowledgment based scheme, to guarantee truthful calculation for the correlations, they propose a homomorphic linear authenticator (HLA) [4] based public auditing architecture that allows the detector to verify the truthfulness of acknowledgments reported by nodes. In neighbor-surveillance based scheme, a Side Channel Monitoring (SCM) [6] scheme to detect selective forwarding attacks in wireless ad hoc networks. SCM use the nodes adjacent to a data communication route, to constitute a side channel for monitoring the forwarding behaviors of the nodes en route. Once misbehaviors are detected, the monitoring nodes send alarm packets to the source node through both channels. Using multi-path routing is also a widely applied technique to minimize the impact of selective forwarding attacks on data delivery rather than detect them. Packet loss can be caused by compromised nodes, outsider jammers, as well as poor radio conditions [1].

A. Disadvantages:

1) Selective forwarding attacks [1] on information integrity and network performance. However, they have limited capability to accurately detect the attacks and identify the compromised sensor nodes.
2) The nodes have limited capability [2] [3] [4] to accurately detect the attacks and identify the compromised sensor nodes [5].
3) The normal packet loss [1] into selective forwarding attack detection for wireless mesh networks.
4) A reputation system is exploited to detect selective forwarding attacks by taking the normal packet loss rate into consideration.

III. SYSTEM ARCHITECTURE

Propose system, a Channel-aware Reputation System with adaptive detection threshold (CRS-A) to detect selective forwarding attacks in WSNs. Specifically, we divide the network lifetime to a sequence of evaluation periods. During each evaluation period, sensor nodes estimate the normal packet loss rates between themselves and their neighboring nodes, and adopt the estimated packet loss rates to evaluate the forwarding behaviors of its downstream neighbors along the data forwarding path. The sensor nodes misbehaving in data forwarding are punished with reduced reputation values by CRS-A. Once the reputation value of a senor node is below an alarm value, it would be identified as a compromised node by CRS-A.

A. Design and Implementation Constraints:

1) WSN consisting of a set of randomly distributed sensor nodes, denoted by N, and a sink node to monitor an open area. Each sensor node periodically senses the interested information from the surroundings, and transmits the sensed data to the sink via multi-hop routing among sensor nodes. Sensor nodes communicate with their neighboring nodes.
2) The cryptographic techniques have been utilized in the network to provide sufficient data confidentiality and authentication against the adversary, then we can focus on resisting selective forwarding attacks.

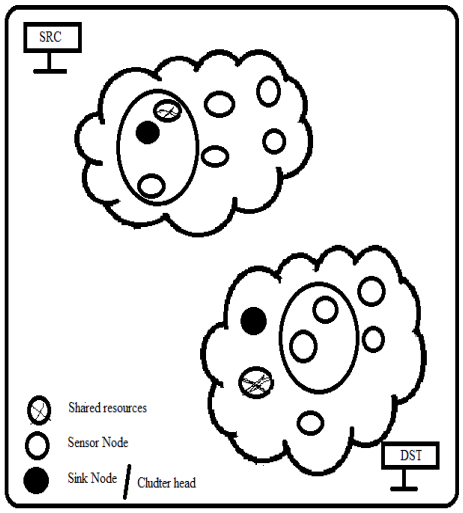

Fig. 3.1: Proposed system (Architecture) and working

3) To detect selective forwarding attacks based on the monitored forwarding traffic information and improve the data delivery ratio for WSNs.

All rights reserved by *www.ijste.org*

1) Design Goals

1) Planned approach towards working - The working in the wireless sensor network will be well planned and organized. The data packet will be securely transferred from source node to destination node, which will help reduce the selective forwarding attacks.
2) Accuracy - The level of accuracy in the proposed system will be higher. All operation would be done correctly and it ensures that whatever information is coming from the center is accurate.
3) Reliability - The reliability of the proposed system will be high due to the above stated reasons. The reason for the increased reliability of the system is that now there would be proper transfer of data packet at destination.
4) No Redundancy - The main objective of proposed system is to prevent data packet from duplication on sensor node. This would assure economic use of storage space and consistency in the data stored.
5) Immediate storage of information - In manual system there are many problems to store the largest amount of information.
6) Easy to Operate - The system should be easy to operate and should be such that it can be developed within a short period of time and fit in the limited budget of the user.

B. Advantages:

1) Evaluates the forwarding behaviors of sensor nodes by utilizing an adaptive detection threshold.
2) A distributed and attack-tolerant data forwarding scheme to collaborate with CRS-A for stimulating the forwarding cooperation of compromised nodes and improving the data delivery ratio of the network.
3) CRS-A with attack-tolerant data forwarding scheme can achieve a high detection accuracy with both of false and missed detection probabilities close to 0, and improve more than 10% data delivery ratio for the network.
4) Less the energy power consumption at data forwarding in this WSN of mobile ad-hoc network.

IV. MATHEMATICAL MODEL FOR PROPOSED WORK

A. Mathematical Model:

1) Normal Packet Loss Estimation: According to the network model, normal packet loss is mainly caused by the poor and unstable wireless channel and MAC layer collisions.

1) Packet Loss Caused by Radio Link Quality: In CRS-A, the link quality estimation for each pair of neighboring nodes is based on the Received Signal Strength Indicator (RSSI) and Signal-to-Noise Ratio (SNR), under the symmetric channel assumption. For each T_t , the packet loss rate caused by poor link quality, denoted by $P_{i,j}(t)$ can be estimated by RSSI and SNR for the transmission link from N_i to N_j.
2) Let n be the number of nodes contending for channel access at N_j and p_t as the probability that a node transmits data in time slot. When MAC channel is at steady state, the probabilities for observing an idle, successful, and colliding slot, denoted as p_i , p_s , and p_c, respectively, are

$$\begin{cases} P_i = (1-P_t)^n \\ P_s = n.P_t.(1-P_t)^{n-1} \\ P_c = 1 - P_i - P_s \end{cases} \quad (1)$$

And the channel busy ratio Rb can be calculated as

$$C_b = 1 - (P_i.t_d)/(P_i.\sigma + P_s.t_s + P_c.t_c) \quad (2)$$

2) Reputation Evaluation: In CRS-A, sensor nodes monitor their neighbors to evaluate reputation scores for their forwarding behaviors during each evaluation period.

$$r_{i,j}^1(t) = \begin{cases} +\delta, \ if \ m_{i,j}(t) \le p_{i,j}(t).S_{i,j}(t) \\ -\delta, \ if \ p_{i,j}(t).S_{i,j}(t) < m_{i,j}(t) \le \xi_{i,j}(t) \\ -\lambda, \ if \ m_{i,j}(t) > \xi_{i,j}(t). \end{cases} \quad (3)$$

where λ is a punishment factor and δ is a adjustment factor. We set $\lambda \gg \delta$ and explain the function as follows.

1) If $m_{i,j}(t) \le p_{i,j}(t).S_{i,j}(t)$, the sampling test is acceptable, which means the transmission between Ni and Nj is successful. Thus, Ni rewards a positive δ to Nj .
2) If $p_{i,j}(t).S_{i,j}(t) < m_{i,j}(t) \le \xi_{i,j}(t)$, we consider it is a normal fluctuation of $P_{i,j}^m$ around pi, j , and rate −δ to Nj to neutralize the reputation evaluation.
3) When $m_{i,j}(t) > \xi_{i,j}(t)$, we consider there is a high probability for Nj to misbehave in the data forwarding. If it happens, Ni rates a punishment −λ to Nj.

3) Reputation Propagation: The negative impacts of mutual reputation promotions among neighboring malicious nodes can be significantly mitigated.

$$r_{i,j}^1(t) = \sum_{x \epsilon NC_{i,g}} \frac{R_{i,x}}{\sum_{s \epsilon NC_i} R_{i,s}} . r_{x,j}^1(t) + \sum_{x \epsilon NC_{i,b}} \frac{R_{i,x}}{\sum_{s \epsilon NC_i} R_{i,s}} . \alpha r_{x,j}^1(t) \quad (4)$$

All rights reserved by *www.ijste.org*

4) Reputation Integration: We calculate the integrated reputation score,

$$R_{i,j} = \begin{cases} R_s, \ if \ R_{i,j} + R_{i,j}^I \leq R_s \\ R_{i,j} + R_{i,j}^I, \ if \ R_s < R_{i,j} + R_{i,j}^I < R_m \\ R_m, \ Otherwise \end{cases} \quad (5)$$

Let us consider S as a system for Adaptive and Channel-aware Forwarding Evaluation during Each Evaluation Period
S= {……

B. Input:

Identify the inputs
F = {f_1, f_2, f_3,……,f_n| 'F' as set of functions to execute commands.}
I = {i_1, i_2, i_3…|'I' sets of inputs to the function set}
O = {o_1, o_2, o_3….|'O' Set of outputs from the function sets}
S = {I, F, O}
I = {Number of sensor node, sink node, nearest nodes, data packet size, transmission rate}
O = {Reduced selective forwarding attack and Updating the reputation of sensor nodes and data forwarding given time period }
F = {Functions implemented to get the output}

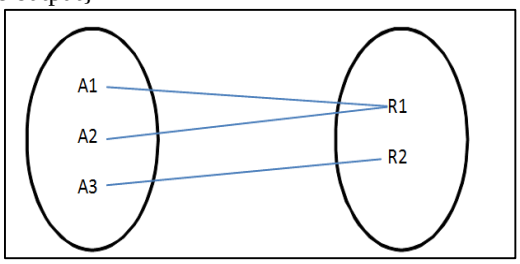

Fig. 4.1: Channel Aware Reputation System Adaptive Routing

A1: 1 Source and 1 Destination I P address
A2: another source communication with same IP
R1: Same source and different Destination IP

5) Algorithmic Details

Adaptive and Channel-aware Forwarding Evaluation during Each Evaluation Period Updating the reputation of sensor nodes and data forwarding during time Input: No. of Nodes N, Source node Ni, Destination node Nj.
There are 3 phases of algorithm:

1) Phase I: Normal Packet Loss estimation.
2) for each Ni ∈ N do
3) Estimate the normal packet loss rate pi, j (t) between Ni and each Nj in Ni 's neighbor set;
4) End
5) Phase II Data Transmission and Monitoring
6) for each Ni ∈ N do
7) Choosing Nj from RCi as the next hop according to Data forwarding ratio (DFR) and the forwarding candidate set of Ni, and use Nj to forward its data;
8) Record the number of sent data packets Si, j (t) and the number of data packets mi, j (t) forwarded by Nj
9) End
10) Phase III Reputation Evaluation and Updating;
11) for each Ni ∈ N do
12) Calculate the attack probability pj of Nj;
13) Determine the optimal detection threshold $\xi_{i,j}^*(t)$ by solving the problem (PP);
14) Evaluate the first-hand reputation score $r_{i,j}^1(t)$;
15) Propagate $r_{i,j}^1(t)$ to its neighboring nodes;
16) if receive propagated reputation scores then
17) Calculate the second-hand reputation score $r_{i,j}^2(t)$;
18) End
19) Calculate the integrated reputation score $R_{i,j}^I(t)$ with $r_{i,j}^1(t)$ and $r_{i,j}^2(t)$ and use it to update Ri, j;
20) end

All rights reserved by *www.ijste.org*

V. REPUTATION SCORE CALCULATION

A. Reputation Evaluation:

In CRS-A, sensor nodes monitor their neighbors to evaluate reputation scores for their forwarding behaviors during each evaluation period by using giv

$$r_{i,j}^{1}(t) = \begin{cases} +\delta, & if\ m_{i,j}(t) \le p_{i,j}(t).S_{i,j}(t) \\ -\delta, & if\ p_{i,j}(t).S_{i,j}(t) < m_{i,j}(t) \le \xi_{i,j}(t) \\ -\lambda, & if\ m_{i,j}(t) > \xi_{i,j}(t). \end{cases}$$

where λ is a punishment factor and δ is a adjustment factor. We set $\lambda \gg \delta$ and explain the function as follows.

- If $m_{i,j}(t) \le p_{i,j}(t).S_{i,j}(t)$, the sampling test is acceptable, which means the transmission between Ni and Nj is successful. Thus, Ni rewards a positive δ to Nj .
- If $p_{i,j}(t).S_{i,j}(t) < m_{i,j}(t) \le \xi_{i,j}(t)$, we consider it is a normal fluctuation of $P_{i,j}^{m}$ around pi, j , and rate −δ to Nj to neutralize the reputation evaluation.
- When $m_{i,j}(t) > \xi_{i,j}(t)$, we consider there is a high probability for Nj to misbehave in the data forwarding. If it happens, Ni rates a punishment −λ to Nj.

B. Reputation Propagation:

The negative impacts of mutual reputation promotions among neighboring malicious nodes can be significantly mitigated.

$$r_{i,j}^{1}(t) = \sum_{x \epsilon NC_{i,g}} \frac{R_{i,x}}{\sum_{s \epsilon NC_i} R_{i,s}} . r_{x,j}^{1}(t) + \sum_{x \epsilon NC_{i,b}} \frac{R_{i,x}}{\sum_{s \epsilon NC_i} R_{i,s}} . \alpha r_{x,j}^{1}(t)$$

C. Reputation Integration:

We calculate the integrated reputation score,

$$R_{i,j} = \begin{cases} R_s, & \text{if } R_{i,j} + R_{i,j}^{I} \le R_s \\ R_{i,j} + R_{i,j}^{I}, & \text{if } R_s < R_{i,j} + R_{i,j}^{I} < R_m \\ R_m, & \text{Otherwise} \end{cases}$$

VI. CONCLUSION

To accurately distinguish selective forwarding attacks from the normal packet loss, CRS-A evaluates the forwarding behaviors by the deviation between the estimated normal packet loss and monitored packet loss. CRS-A can achieve a high detection accuracy with low false and missed detection probabilities, and the proposed attack tolerant data forwarding scheme can improve more than 10% data delivery ratio for the network.

VII. FUTURE SCOPE

As future work, the proposed system will be improved for less energy consumption in mobile ad-hoc network. In future investigation into 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.

ACKNOWLEDGMENTS

We would like to thank Dr. P.N. Mahalle and Dr. A. V. Deshpande for their comments on this paper and the help in early discussion of this work. We thankful to our organization Smt. Kashibai Navale College of Engineering, Vadgaon (BK), Pune which gives us opportunity to work over this paper.

REFERENCES

[1] 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.
[2] 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.
[3] 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.
[4] T. Shu and M. Krunz, "Detection of malicious packet dropping in wireless ad hoc networks based on privacy-preserving public auditing," in Proc.5th ACM Conf. Security Privacy Wireless Mobile Netw. (WiSec), 2012, pp. 87–98.
[5] S. Marti, T. J. Giuli, K. Lai, and M. Baker, "Mitigating routing misbehavior in mobile ad hoc networks," in Proc. ACM MobiCom, 2000, pp. 255–265.

All rights reserved by *www.ijste.org*

[6] X. Li, R. Lu, X. Liang, and X. Shen, "Side channel monitoring: Packet drop attack detection in wireless ad hoc networks," in Proc. IEEE Int. Conf. Commun. (ICC), 2011, pp. 1–5.
[7] T. Shu, M. Krunz, and S. Liu, "Secure data collection in wireless sensor networks using randomized dispersive routes," IEEE Trans. Mobile Comput., vol. 9, no. 7, pp. 941–954, Jul. 2010.
[8] A. Liu, Z. Zheng, C. Zhang, Z. Chen, and X. Shen, "Secure and energy efficient disjoint multipath routing for WSNs," IEEE Trans. Veh. Technol., vol. 61, no. 7, pp. 3255–3265, Sep. 2012.
[9] J. Ren, Y. Zhang, K. Zhang, and X. Shen, "Exploiting mobile crowdsourcing for pervasive cloud services: Challenges and solutions," IEEE Commun. Mag., vol. 53, no. 3, pp. 98–105, Mar. 2015.
[10] J. Tang, Y. Cheng, and W. Zhuang, "Real-time misbehavior detection in IEEE 802.11-based wireless networks: An analytical approach," IEEE Trans. Mobile Comput., vol. 13, no. 1, pp. 146–158, Jan. 2014.

All rights reserved by *www.ijste.org*