ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 6, Issue 3, March 2018

Exploiting Channel-Aware Reputation System against Malicious Packet Dropping in WSNs

Pranali Shekokare [1], Dr. S.K Pathan [2]

P.G. Student, Department of Computer Engineering, Smt. Kashibai Navale College of Engineering, Pune, Maharashtra, India[1]

Professor, Department of Computer Engineering, Smt. Kashibai Navale College of Engineering, Pune, Maharashtra, India[2]

ABSTRACT: Numerous WSNs are deployed in unattended and even unfriendly conditions to perform mission-basic assignments, for example, combat zone observation and country security checking. This paper 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. Though the changeable wireless channel in WSNs, the packet loss rate throughout 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 classifies the data forwarding behaviours of sensor nodes, by supervising the packet loss and the estimated normal loss. Optimize the detection accuracy of CRS-A, using optimal threshold for forwarding assessment. Although ,an attack-tolerant data forwarding method is developed to participate with CRS-A for encouraging the forwarding cooperation of arbitrary nodes and increasing the data delivery ratio of the network. Contribution work is in this CRS-A system, providing the authentication of nodes in the multi-hop dynamic source routing in wireless sensor network. Another one is, saves the energy of sensor nodes within the detection of malicious node and forward data packet in mobile ad-hoc network. Commitment work is in this CRS-A framework, amass key pre-appropriation conspire usage, with the end goal that there is an exceptional key, called path key, to ensure information transmitted in the whole steering way. Another one is, saves the energy of sensor nodes within the detection of malicious node and forward data packet in mobile ad-hoc network.

KEYWORDS**:** Channel-Aware, Group Key, Multi-Hop Routing, Packet Dropping, Reputation System, Selective Forwarding Attack, Side Channel Monitoring, Wireless Sensor Network.

I. INTRODUCTION

Wireless sensor network (WSN) has been broadly utilized for security monitoring and information gathering procedure in both military and non-military personnel applications. Because of the absence of physical assurance, sensor nodes are easily compromised by attackers, making WSN unsafe to various security threats. In selective forwarding attacks, malicious nodes behave like normal nodes and selectively drop packets in the whole sensor network communication. The variety of defense approaches against selective forwarding attack is overwhelming. 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 increase the network performance. In this paper, we propose a Channel-aware Reputation System with adaptive detection threshold (CRS-A) to detect selective forwarding attacks in WSNs. There are two ways of accuracy detection in WSN: One is, detecting accurate malicious node in data forwarding shortest path and the other is, normal nodes cannot be wrongly detect as malicious node. Thus data forwarding ratio is improved in WSN.

DOI: 10.15680/IJIRCCE.2018.0603003

II. RELATED WORK

Mitigating routing misbehaviour in mobile ad hoc networks [1] paper, watchdog identifies misbehaving nodes and Pathrater that helps routing protocols to avoid these nodes. Advantages are: To increase throughput by 17%.Benefitted when increasing the no. of routing nodes while minimize the effect of misbehaving nodes. Disadvantages are: Performance is low. The paper [2] proposes the 2ACK scheme technique for routing schemes to detect routing misbehaviour. The 2ACK scheme is to send two-hop acknowledgment packets in the opposite direction of the routing path. Advantages are: Reliable data transmission. Reliable route discovery, limited transmission power, limited overhearing range. Disadvantages are: Time consumption during to detect routing misbehavior.

The paper [3] proposes scheme CHEMAS (CHEckpoint-based Multi-hop Acknowledgement Scheme), a lightweight security scheme for detecting selective forwarding attacks. Proposed system implements for randomly select part of intermediate nodes along a forwarding path as checkpoint nodes which are responsible for generating acknowledgements for each packet received. Advantages are: A simple and efficient security scheme for detecting selective forwarding attacks. Reduce the communication overhead in each sensor node. Save the energy consumption in data forwarding. Disadvantages are: Packet loss can be caused by compromised nodes, outsider jammers, as well as poor radio conditions. In [4] paper, that generate randomized multipath routes. Under the design, the routes taken by the “shares” of different packets change over time. Advantages are: Security Performance is high. Cost of energy reasonable. Disadvantages are: Expensive to simulate.

The paper [5] describes proposed system, side channel monitoring (SCM) technique to detect packet drop attack in ad hoc networks SCM use two channels: primary channel and side channel.SCM is able to detect the cooperative attacks and involves local communication only. Advantages are: Involves local communication only. Also find collaborative attack. Disadvantages are:Can’t generate alarm message for partial dropping . No encryption technique to secure the channel. In [6] paper, proposed an energy efficient node disjoint multipath routing for wireless sensor network in order to provide efficient energy utilization for sensor nodes and maximize the lifetime of the senor network. Advantages are: Performance is better in network lifetime.Average energy consumption, control on packet overhead. Average packet delivery ratio.

The paper [7] represents a homomorphic linear authenticator(HLA) based public auditing architecture that allows the detector to verify the truthfulness of the packet loss information reported by nodes. The proposed system, achieves better detection accuracy. Advantages are:To improve the detection accuracy, we propose to exploit the correlations between lost packets. It provides privacy preserving on packet. Disadvantages are: Large computational overhead on source node. The paper [8] elaborates the EAACK technique is based on acknowledgement so it is very necessary to that all acknowledgment packets in EAACK are authentic. Advantages are: Packet delivery ratio is high. Throughput is high. End-to-end packet delivery delay is average. Performance is positive.It provides security. Disadvantages are: If collision occurred then time consumption in packet delivery at receiver side.

In [9] paper, proposes a novel real-time hybrid share(HS) misbehaviour detector for IEEE 802.11e based wireless local area networks (WLANs). The detector keeps updating its state based on every successful transmission and makes detection decisions by comparing its state with a threshold. Advantage is: Performance is better. The[10]paper investigated the mobile crowd sourcing architecture, and presented technical challenges with possible solutions to facilitate the implementation and development of mobile crowd sourcing. Advantages are: Location of task independent of seeker’s location. Retrieving tasks with manually entered location. Disadvantages are: Priority-1 tasks are assigned to one solver only. No location based history. Privacy issues.

III. PROPOSED ALGORITHM

The proposed system a Channel-aware Reputation System with adaptive detection threshold (CRS-A) to detect selective forwarding attacks and identify malicious nodes. In CRS-A, each sensor node maintains a reputation table to evaluate the long-term forwarding behaviours of its neighbouring nodes. The reputation update in CRS-A consists of three procedures: reputation evaluation, propagation and integration. The normal packet loss estimation, reputation evaluation, propagation and integration are getting by calculating reputation scores and update in reputation table and finally detect the malicious node. After detection of malicious node we implement attack tolerant data forwarding technique. Then, this system is very useful in data sensitive applications, for example, health-care organizations and industry monitoring applications.

The 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 neighbouring nodes, and adopt the estimated packet loss rates to evaluate the forwarding behaviours of its downstream neighbours 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.

Advantages :

1. Ascertains the sending practices of sensor nodes by utilizing an adaptive detection threshold.
2. A dispersed and attack tolerant information sending plan to work together with CRS-A for empowering the sending collaboration of traded off nodes and enhancing the information conveyance proportion of the system.
3. CRS-A with attack tolerant information sending system can achieve a high identification precision with both of false and missed discovery probabilities near 0, and enhance more than 10 rate information conveyance proportion for the system.
4. Reduced energy power usage at data sending in this WSN.
5. It has better security performance due to group key assigned to shortest path nodes.

IV. PSEUDO CODE

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:

```
Phase I: Normal Packet Loss estimation.
for each Ni ∈N do
    Estimate the normal packet loss rate pi, j (t) between Ni and each Njin Ni 's neighbor set;
End
Phase II Data Transmission and Monitoring
for each Ni ∈N do
    Choosing Nj from RCias the next hop according to Data forwarding ratio (DFR) and the forwarding candidate set of Ni, and use Njto forward its data;
    Record the number of sent data packets Si, j (t) and the number of data packets mi, j (t) forwarded by Nj
End
Phase III Reputation Evaluation and Updating;
for each Ni ∈N do
    Calculate the attack probability pjof Nj;
    Determine the optimal detection threshold $\xi^{*}_{i,j}(t)$by solving the problem (PP);
    Evaluate the first-hand reputation score $r^{1}_{i,j}(t)$;
    Propagate $r^{1}_{i,j}(t)$to its neighboring nodes;
    if receive propagated reputation scores then
        Calculate the second-hand reputation score $r^{2}_{i,j}(t)$;
    End
    Calculate the integrated reputation score $R^{I}_{i,j}(t)$with $r^{1}_{i,j}(t)$and $r^{2}_{i,j}(t)$and use it to update Ri, j;
End
```

V. SIMULATION RESULTS

Experimental evaluation result to compare the proposed system with the existing system for evaluating the performance .The simulation platform used is built using Java language (version jdk 8) on Windows platform. The system does not require any specific hardware to run; any standard machine is capable of running the application.

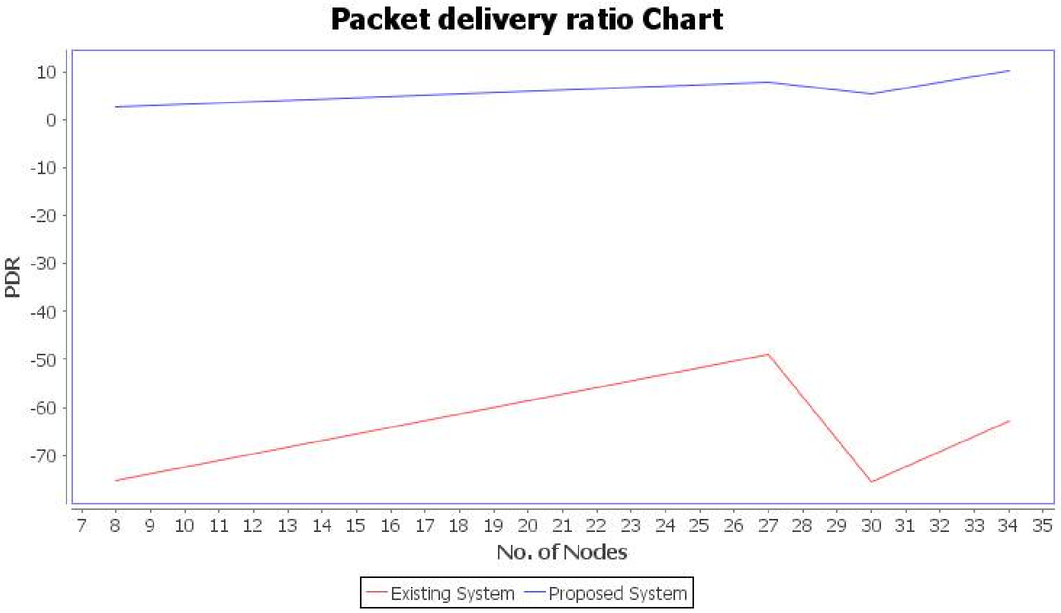

Fig. Comparative graph of packet delivery ratio (PDR) for WSN.

By observing the above graph we can conclude that the proposed system gives better results as compared to the existing system in terms of various parameters calculated. The packet loss ratio and throughput results are not up to the expectations but they can be further improved. But the overall results are on target.

VI. CONCLUSION AND FUTURE WORK

At the endeavour the proposed CRS-A system to detect selective forwarding attacks in WSNs showing through simulation. To precisely distinguish selective forwarding attacks from the normal packet loss, CRS-A assesses the forwarding behaviours by the deviation between the estimated normal packet loss and monitored packet loss. CRS-A can accomplish high detection accuracy with low false and missed detection probabilities, and the proposed attack tolerant data forwarding method can improve more than 10%data delivery ratio for the network. As future work, the proposed framework will be enhanced for less energy utilization in mobile ad-hoc network. In future examination 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 evaluate due to the mobility of sensor nodes.

REFERENCES

1. 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.
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. 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. 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.
5. 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.
6. 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.
7. 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.
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. 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.
10. J. Ren, Y. Zhang, K. Zhang, and X. Shen, "Exploiting mobile crowd sourcing for pervasive cloud services: Challenges and solutions," *IEEE Commun. Mag.*, vol. 53, no. 3, pp. 98–105, Mar. 2015.
11. R. H. Akbani, S. Patel, and D. C. Jinwala, "DoS attacks in mobile ad hoc networks: A survey," in Proc. 2nd Int. Meeting ACCT, Rohtak, Haryana, India, 2012, pp. 535–541.
12. T. Anantvalee and J. Wu, "A Survey on Intrusion Detection in Mobile Ad Hoc Networks," in Wireless/Mobile Security. New York: Springer- Verlag, 2008.