ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

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

Visit: www.ijirset.com

Vol. 7, Issue 6, June 2018

Channel-Aware Reputation Evolution System to Detect Malicious Nodes in WSN's

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: Different WSNs are passed on in unattended and even threatening conditions to perform mission-fundamental assignments, for example, fight zone discernment and country security checking.This paper takes a particular kind of DoS attack known selective forwarding attacks that can noxiously drop a subset of sending packets to degenerate framework execution and dependability. Regardless of the way that the alterable remote occupy in WSNs, the package disaster rate all through the correspondence of sensor nodes may be high and distinction from time to time. In this paper, we propose a channel-aware reputation structure with adaptable detection edge (CRS-A) to recognize pernicious nodes which selectively drop packets in WSNs.The CRS-A recognizes the information sending practices of sensor nodes, by regulating normal loss and evaluated ordinary loss. Optimize the detection accuracy of CRSA, using optimal threshold for forwarding assessment . In spite of the fact that an attack tolerant information sending technique is produced to take an interest with CRS-A for empowering the sending participation of subjective nodes and expanding the information conveyance proportion of the system. 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 extensively utilized for security checking and information gathering system in both military and non-military staff applications. In perspective of the nonappearance of physical assertion, sensor nodes are easily exchanged off by attackers, making WSN unsafe to various security threats. In selective forwarding attacks pernicious nodes carry on like ordinary nodes and specifically drop packets in the entire sensor network. The variety of protect approaches against selective forwarding attack is overpowering. It in like manner has basically negative impacts to data trustworthiness, especially for data tricky applications. Therefore, it is outstandingly trying to recognize the specific sending attacks and augmentation the framework execution. In this paper, we propose a Channel-aware Reputation System with adaptive detection threshold (CRS-A) to recognize malicious nodes which selectively drop packets 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.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

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

Visit: www.ijirset.com

Vol. 7, Issue 6, June 2018

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 SYSTEM

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

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

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

Visit: www.ijirset.com

Vol. 7, Issue 6, June 2018

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.

Mathematical Model

I. 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

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

II. 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 $\lambda$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* .

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

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

Visit: www.ijirset.com

Vol. 7, Issue 6, June 2018

• If $p_{i,j}(t).S_{i,j}(t) < m_{i,j}(t) \leq \xi_{i,j}(t)$, we consider it is a normal fluctuation of $P_{i,j}^{m}$around *pi, j* , and rate $-\delta$ 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 $-\lambda$ to *Nj*.

III. Reputation Propagation

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

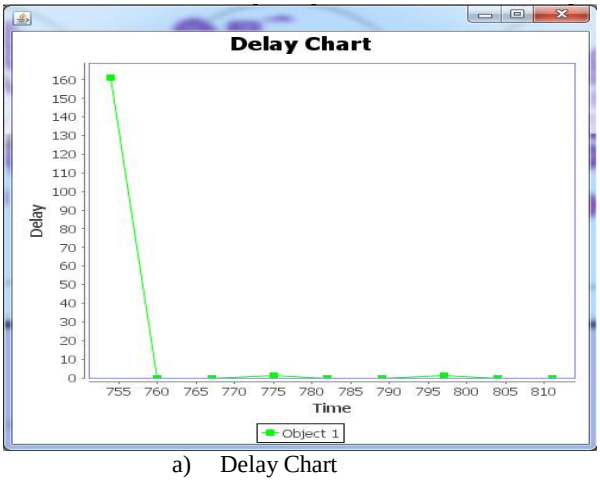
$$r_{i,j}^{1}(t) = \sum_{x \epsilon NC_{i,g}} \frac{R_{i,x}}{\sum_{s \epsilon NC_i} R_{i,s}} . r_{x,j}^{1}(t) + \sum_{x \epsilon NC_{i,b}} \frac{R_{i,x}}{\sum_{s \epsilon NC_i} R_{i,s}} . \alpha r_{x,j}^{1}(t) \quad (4)$$

IV. Reputation Integration

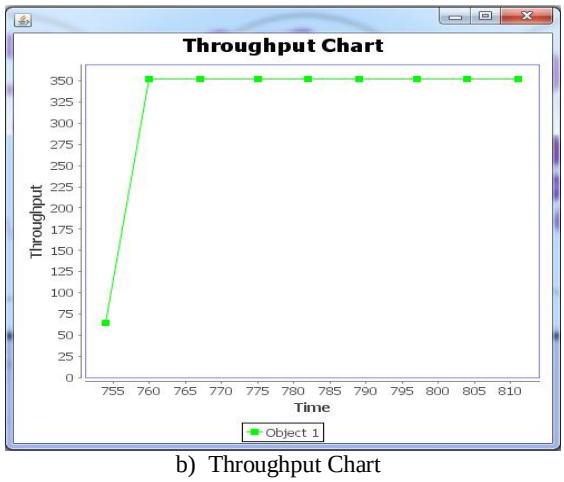
We calculate the integrated reputation score,

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

IV. EXPERIMENTAL RESULTS



a) Delay Chart



b) Throughput Chart

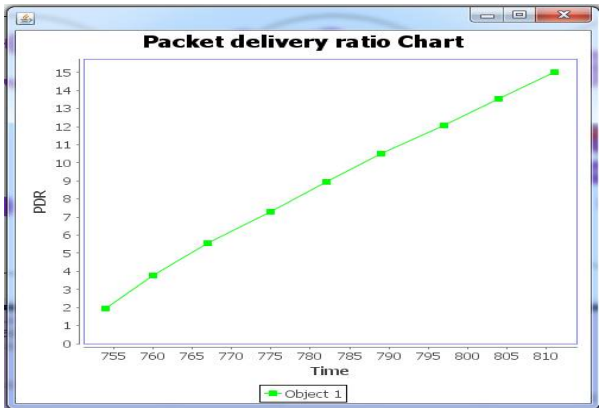
ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

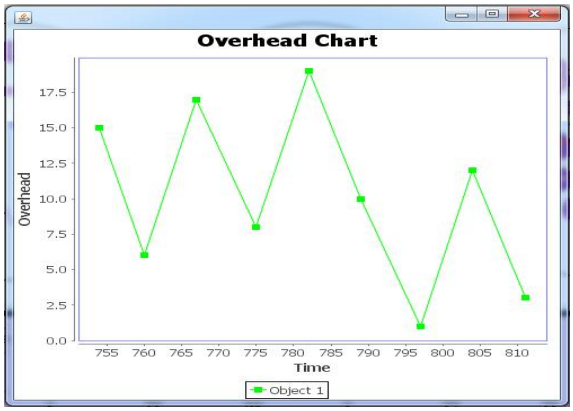
(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

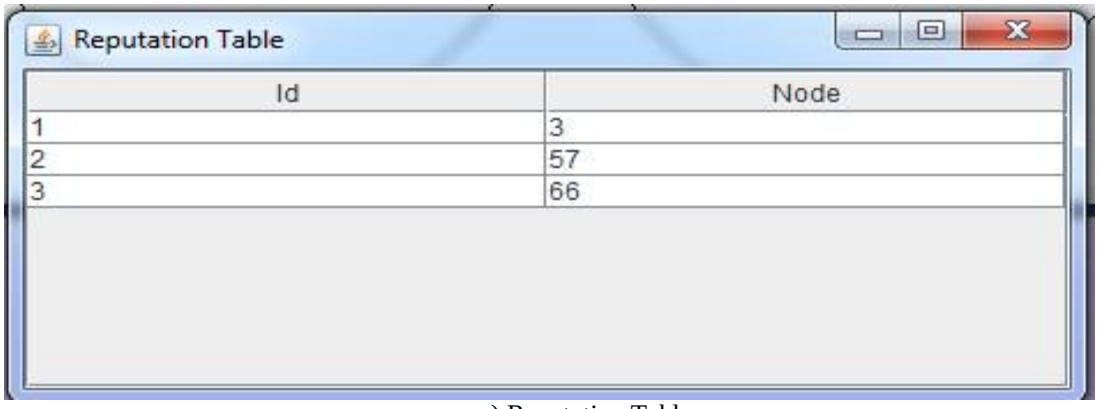
Vol. 7, Issue 6, June 2018



b) Packet Delivery Ratio Chart



d) Overhead Chart



e) Reputation Table

By observing the above graphs we can conclude that the proposed system gives better results as compared to the existing system in terms of various parameters calculated. We can see overall results are on target. Reputation Table shows the entry of malicious nodes.

V. FUTURE ENHANCEMENT

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 investigation, since the normal packet loss rate is more fluctuant and difficult to evaluate due to the mobility of sensor nodes.

VI. CONCLUSION

At the endeavour the proposed CRS-A system to recognize selective forwarding attacks in WSNs showing through simulation. To absolutely recognize selective forwarding attacks from the normal packet loss, CRS-A surveys the sending behaviours by the deviation between the assessed ordinary data loss and observed data loss. CRS-A can achieve high discovery exactness with low false and missed recognition probabilities, and the proposed attack tolerant information sending strategy can enhance more than 10 rate data delivery proportion for the network.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

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

Visit: www.ijirset.com

Vol. 7, Issue 6, June 2018

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] 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.