Anti Malicious Threshold System

Krishna. A Kumar*, Vinu Ramdhas**

*Electronics And Communication, Toc H institute of Science And Technology
**Electronics And Communication, Toc H institute of Science And Technology

***Abstract*-** WSNs are spatially distributed autonomous sensors to monitor physical or environmental conditions such as temperature sound pressure etc. They are highly prone to malicious attacks and security threats[12][13] since their structures are not predetermined. Malicious attack on the sense that it makes the sensor nodes to drop the packets of data when moved from one node to another. This will surely degrade the performance of the whole system. Another major issue is to distinguish malicious attack from normal packet loss. Most cases we fail to realize malicious attack from normal packet loss. In order to overcome that problem we adopt a new method using threshold value called Channel Aware Anti Malicious Threshold System(CAMTS).

***Index Terms*-** WSNs; malicious; packet loss; CAMTS

I.INTRODUCTION

As a promising area in the future the wireless sensor network helps us to gather information from remote areas since they are sparsely deployed. The structure of WSNs are not predetermined. The size of the WSNs can be varied from grain to medium carton box. The advantages of WSNs mainly in military, health care and in environmental scenarios. In military applications it helps to collect information on mine bombs pitted by enemy army. It is easy to find the accurate target of enemies in war zone. Biological and chemical attacks also can be monitored. The intrusion of enemy troops during night can be determined by using thermal variations on the human bodies with the help of WSNs. Since it does not have a predetermined structure, it is easily prone to attacks. Meanwhile neighboring nodes will not be aware of the attack. Thus pack forwarding will be done while it is under the attack and the amount of packet drop also will be high. The sensor nodes[10][11] in hostile conditions should be considered serious. Since it is in hostile environment the packet loss can be occurred not only due to malicious attack but can be occurred due to bad and unreliable channel conditions.

II. METHODOLOGY

Consider 15 data packets for the time being and nodes; source node N_s, node N_a ,node N_b ,destination node N_d. Source node transfer data packets to destination node through intermediate nodes N_a and N_b and N_b performs better than a during normal packet transfer. If N_a transfers 8 data packets to N_d while if N_b transfers only 3 packets to N_d then we can conclude that the performance of N_a is greater than N_b and N_b has undergone a malicious attack.

The method can be done as considering source node N_s destination node N_d and intermediate nodes N_a N_b N_c N_d etc. The value of intermediate nodes can be determined by DFR-Data Forwarding Ratio. As the amount of packet forwarding from one node to another is high that is with less packet loss then the DFR is high and node with high DFR can be considered as dependable node for the data forwarding from source to destination.

The performance can be evaluated as Reputation Evaluation Reputation Propagation Reputation Integration with 50 numbers of nodes**.** The proposed method works on the threshold value (probability value) 21 in reputation evaluation. This value is obtained by the graph coinciding point of normal packet loss and malicious packet loss to probability.

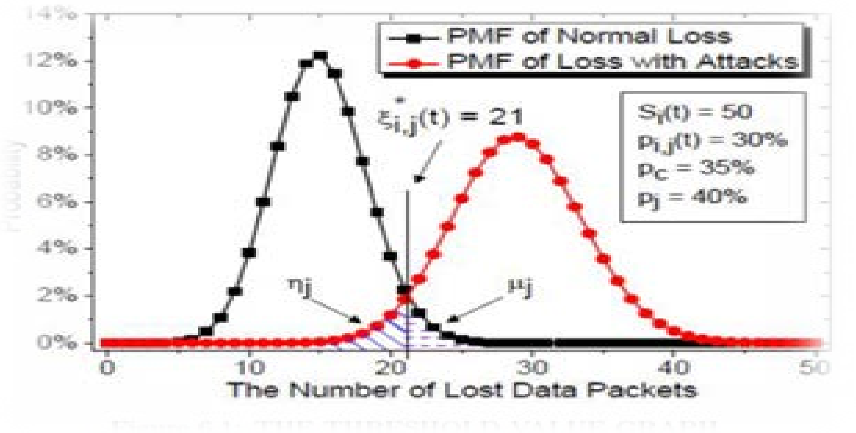

Fig.1. Gaining the threshold value

III. LITERATURE SURVEY

Most of the related works are on to lessen the effect of malicious attack or to give an alarm on malicious attack. The related works can be biased into acknowledgement based and neighbor surveillance based. In acknowledgment based; Xiao.et.al. [1] introduces a method where it selects randomly intermediate nodes significantly increases the resilience against attacks. This scheme could be used to transfer ordinary packets, but when the source node generates a very important packet, it should be delivered to the base station through multiple paths. Marti et.al [2] throughput: this is the percentage of sent data packets actually received by the intended destination. False positives occur when the watchdog mechanism reports that a node is misbehaving. Only initial work has taken to detect the malicious nodes. No solution for their problem. Watch dog is ineffective to cooperative attacks. Liu et.al. [3] The 2ACK technique is based on a simple 2-hop acknowledgment packet that is sent back by the receiver of the next-hop link. How to derive the triplet information so that the 2ACK sender and the observing node are informed of such information. Knowledge of topology of the 2-hop neighborhood may be used. Ozdemir et.al.[4] Protocol RDAT improves the reliability of aggregated data by evaluating sensor nodes and data aggregators via appropriate functional reputations. Consumption of energy is not even in the whole network. The protocol is simple having high protocol cost, and difficult implementation. Djahel et.al.[5] The packet dropping attack, which is known as one of the most destructive threats in MANETs, and illustrates in depth the different schemes used by adversaries targeting on both reactive and proactive protocols. Most of the proposed solutions are built on a number of assumptions which are either hard to realize in a hostile and energy constrained environment like MANETs. Li et.al.[6] SCM is able to detect attackers acting as a team. Unlike the version of Watchdog extended to co-operative attacks, SCM does not require trusted nodes (thus no additional hardware investment) and involves only local communication (thus more efficient). It fails when more than two malicious nodes are colluding in a row. For example, three malicious nodes one next to another act as a team to drop packets along a data communication path. Hao et.al.[7] By utilizing the game theoretic approach, we analyze the collusion in selective forwarding attacks. The selective forwarding attack is launched from inside of the network. Joshi et.al.[8] This system has a powerful attack control, which is one of the necessary conditions to guarantee the data security. Once the activator defines the keys to the nodes, the priority will be generated automatically. Ambiguous collision Receiver collision Limited transmission power False misbehavior report Collusion Partial dropping.

IV. DESIGN GOALS

A. Accurate detection: The detection of malicious nodes must be accurate and should be false proof. The forwarding of the data packets from source to destination is through the intermediate nodes. In some cases we may falsely accuse normal nodes as malicious nodes. This may lead to the loss of well working nodes. This may result in no cost effect.

B. Improvement in Packet Delivery Ratio: The packet delivery from one node to another especially among intermediate nodes must be high. The nodes with high DFR will be allowed to participate in data/packet propagation process from source to destination. With high DFR/path[14][15] it shows that the nodes are least prone to malicious and highly dependable.

IV. EVALUATION PROCESSES

A. REPUTATION EVALUATION

We forward the data packets to all 50 nodes. Thus if packet loss from one to another exceeds 21 then the node that transferred data can be considered as malicious. By this method we find DFR value. That is if the amount of data forwarding to next node from a node is high from the data received, then the DFR is good and that node is considered as good for communication. Each node has unique value of DFR and they assigned as +**δ**, –**δ**, ⋋.

δ- adjustment factor; +1

⋋-punishment factor; -1

$$r^{1}_{i,j=}\begin{cases} +\boldsymbol{\delta}\text{- if packet loss is less than probability value 21} \\ -\boldsymbol{\delta}\text{- if packet loss slightly high than probability value 21} \\ \leftthreetimes\text{-if loss is very much higher than probability value 21} \end{cases}$$

This information is send to neighboring nodes of every node.

B. REPUTATION PROPAGATION

The second hand reputation is done for source and destination nodes. Along with adjustment factor, the values are also distributed to the neighbors. The second hand reputation is calculated as reputation value/ score of source node;

$$\frac{\mathit{Sum\ of\ reputation\ scores\ of\ 4\ neighboring\ nodes}}{\mathit{number\ of\ neighboring\ nodes}}$$

That is if 2, 5,8,13 are neighboring nodes of source node(say for the time being) and they have their own of reputation scores[9]. To find among them, the honest and dishonest nodes, we calculate the second hand reputation scores. We take node 8. Then to find whether it is honest /dishonest

If calculated value is less than $r^{2}_{i,j}$ (which is first hand long term reputation score) then it is honest.

If calculated value is greater than $r^{2}_{i,j}$ then it is dishonest.

$$r^2_{i,j} = \frac{\text{sum of reputation scores of 4 nodes}}{\text{number of nodes}(2,5,8,13)} * r^1_{x,j} + \frac{\text{sum of reputation scores of 4 nodes}}{\text{number of nodes}(2,5,8,13)} * \alpha * r^1_{x,j}$$

where $r^1_{x,j}=1$.

In order to reduce the malicious nature of the dishonest nodes we multiply a factor called penalty factor **α** were the value of **α** is 0.6. As the negativity of the malicious nodes get reduced to normal value these nodes can be made to participate in data transfer from one node to another in future.

C. REPUTATION INTEGRATION

Reputation integration is a combination of reputation evaluation and reputation propagation. The reputation table is updated on the basis of the first-hand and second-hand reputation scores.

$R^1_{i,j}(t)= \sigma*r^1_{i,j}(t)+(1-\sigma)*r^2_{i,j}(t)$

σ =0.75, weight factor.

V. MALICIOUS NODE IDENTIFICATION

Even after nodes undergone these processes there still might be nodes with malicious behavior. In order to identify them we introduce alarm reputation value R_a. If calculated value of nodes is less than R_a then it is purely malicious. If calculated value is greater than R_a then it is normal node.

$R^1_{i,j} > R_a$ – normal node

$R^1_{i.j} < R_a$ – highly malicious node (therefore completely avoided)

VI. RESULTS

The results are obtained with the help of NS2 (Network Simulation – Version2) software. The result shows that with the Channel Aware Anti Malicious Threshold System the data propagation delivery of packets from source to destination during normal mode and under malicious attack mode are almost same and can be achieved as former.

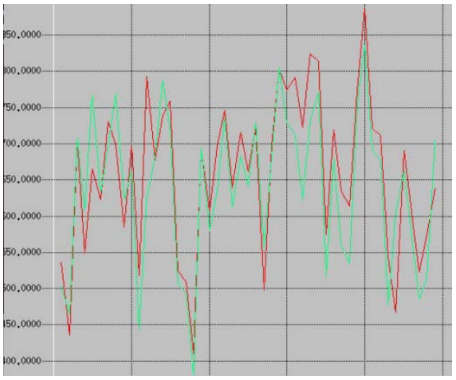

Fig. 2. Graph of no. of nodes vs packet delivery ratio

ACKNOWLEDGMENT

This paper is supported by Wireless Technology stream of Electronics and Communication Department of Toc h Institute of Science And Technology, India. I sincerely pay my gratitude to my guide and staff of my institution for helping me to accomplish the task of topic presentation.

REFERENCES

[1] B. Xiao, B. Yu, and C. Gao, “Chemas: Identify suspect nodes in selective forwarding attacks,” J. Parallel Distributed Comput., vol. 67, no. 11, pp.1218–1230, 2007.

[2] 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.

[3] K. Liu, J. Deng, P. Varshney, and K. Balakrishnan, “An acknowledgment-based approach for the detection of routing misbehavior in manets,” IEEE Trans. Mob. Comput., vol. 6, no. 5, pp. 536–550, 2007.

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

[5] S. Djahel, F. Nait-Abdesselam, and Z. Zhang, “Mitigating packet dropping problem in mobile ad hoc networks: proposals and challenges,” IEEE Commun. Surv. & Tutor., vol. 13, no. 4, pp. 658–672, 2011.

[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 ICC, 2011, pp. 1–5.

[7] D. Hao, X. Liao, A. Adhikari, K. Sakurai, and M. Yokoo, “A repeated game approach for analyzing the collusion on selective forwarding in multihop wireless networks,” Comput. Commun., vol. 35, no. 17, pp. 2125–2137, 2012.

[8] E. Shakshuki, N. Kang, and T. Sheltami, “Eaacka secure intrusiondetection system for manets,” IEEE Trans. Ind. Electro., vol. 60, no. 3,pp. 1089–1098, 2013.

[9] H. Lin, X. Zhu, Y. Fang, D. Xing, C. Zhang, and Z. Cao, “Efficient trust based information sharing schemes over distributed collaborative networks,” IEEE J. Sel. Areas Commun., vol. 31, no. 9, pp. 279–290, 2013.

[10] X. Liang, X. Lin, and X. Shen, “Enabling trustworthy service evaluation in service-oriented mobile social networks,” IEEE Trans. Parallel Distr.Sys., vol. 25, no. 2, pp. 310–320, 2014.

[11] J. Ren, Y. Zhang, K. Zhang, and X. Shen, “Sacrm: Social aware crowdsourcing with reputation management in mobile sensing,” Computer Commun., vol. 65, no. 15, pp. 55–65, 2015.

[12] I. Butun, S. Morgera, and R. Sankar, “A survey of intrusion detection systems in wireless sensor networks,” IEEE Commun. Surv. & Tutor.,vol. 16, no. 1, pp. 266–282, 2014.

[13] Y. Zou, X. Wang, and W. Shen, “Physical-layer security with multiuser scheduling in cognitive radio networks,” IEEE Trans. Commun., vol. 61, no. 12, pp. 5103–5113, 2013.

[14] B. Xiao, B. Yu, and C. Gao, “Chemas: Identify suspect nodes in selective forwarding attacks,” J. Parallel Distributed Comput., vol. 67, no. 11, pp.1218–1230, 2007.

[15] D. Hao, X. Liao, A. Adhikari, K. Sakurai, and M. Yokoo, “A repeated game approach for analyzing the collusion on selective forwarding in multihop wireless networks,” Comput. Commun., vol. 35, no. 17, pp.2125–2137, 2012.

AUTHORS

First Author – Krishna. A Kumar, M.tech Student, Toc H Institute of Science and Technology, krishnaanilkr@gmail.com.

Second Author – Vinu Ramdhas, Asst. Prof., Toc H Institute of Science and Technology,vinur81@gmail.com.