Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 63 (2015) 183 – 188

Procedia Computer Science

6th International Conference on Emerging Ubiquitous Systems and Pervasive Networks, EUSPN-2015

Neighbor Node Trust Based Intrusion Detection System for WSN

Syed Muhammad Sajjad[a], Safdar Hussain Bouk[b], Muhammad Yousaf[a]

[a]*Riphah Institute of Systems Engineering, Riphah International University, Islamabad, Pakistan*
[b]*Department of Electrical Engineering, Comsats Institute of Information Technology, Islamabad, Pakistan*

Abstract

Timely detection of anomalous activity in wireless sensor network is critical for the smooth working of the network. This paper presents an intrusion detection technique based on the calculation of trust of the neighboring node. In the proposed IDS, each node observes the trust level of its neighboring nodes. Based on these trust values , neighboring nodes may be declared as trustworthy, risky or malicious. Trustworthy nodes are recommended to the forwarding engine for packet forwarding purposes. The proposed scheme successfully detects Hello flood attack, jamming attack and selective forwarding attack by analyzing the network statistics and malicious node behavior. The simulation results show that network performs better when neighbor node trust management based anomaly detection technique is in place.

Peer-review under responsibility of the Program Chairs

Keywords: Intrusion Detection System; Risk; Trust; Trusted Node; Wireless Sensor Network

1. Introduction

Wireless Sensor Network (WSN) is an emerging notion and has gained enormous diligence of the research community due to increasing modernization of the technology. WSN is a self-organized network of large number of low power and low cost sensor nodes[1]. These sensor nodes are light-weight and movable devices having capabilities of sensing, communicating and processing the information to the targeted user. They have limited transmission range and communicate directly with nodes lies within its transmission range. Communication with a far end node is performed via intermediate node. Sensor networks are susceptible of exterior and interior outbreaks[2 3 4]. Motes often lacks the ability of dealing a tough attacker owing to its resource constraints nature. In this case secondary level of defense often called intrusion detection system is required[5 6 7]. Exploitation of efforts by the attacker can be detected with the help of intrusion detection system. The confidence and faith of a node in the ability, consistency and trustworthiness of other nodes is termed as trust[8]. Trust based on direct observation of a node is also called direct trust or first-hand information. A node's observation and opinion about other nodes based on their earlier performances in an explicit

* Corresponding author. Tel.: +92-51-8438377 ; fax: +92-51-8438376.
E-mail address: muhammad.sajjad@riu.edu.pk

Peer-review under responsibility of the Program Chairs
doi:10.1016/j.procs.2015.08.331

perspective on a certain period of time is termed as reputation[9 10 11]. Reputation is also called indirect trust or second hand information[12 13 14]. This paper elaborates a neighbor node trust calculation and evaluation based anomaly intrusion detection technique. Remaining of the paper is structured as follows: Section II covers the related work. Section III provides the detailed phases of the proposed scheme. It presents the system model and the initial observations of the nodes in the network. Discussion about the components and blocks of the proposed solution is also carried out in this section. Results are discussed in section IV. Finally, section V concludes the paper.

2. Related Work

The idea of trust computation based intrusion detection systems originates with the design of an IDS by Wang et al.[15] for mobile ad hoc networks (MANETs) based on trust variations and chain of evidence. The assessment of the network node is carried out periodically. A trust assessment and reputation interchangeability based intrusion detection method is offered by Ebinger et al.[16]. The combination of reputation, trust and confidence with trustworthiness cause an improvement in the detection of intrusion. Various trust management mechanisms[17 18 19] have also been presented for WSN. The primary objectives of these techniques include security of systems and reliability of the information. A trust based IDS is proposed by[20] for cluster WSN. Cluster head (CH) performs the trust calculation and evaluation of nodes present in the cluster. Honesty (social trust) and supportiveness as well as energy consumptions (quality of service trust) are the assessment metrics used by the authors for the absentness and identification of malicious activity. Base station evaluates the trust level of cluster head (CH). Fuzzy logic in combination of evidence theory based IDS is presented in[21]. Behavior of nodes is observed and malicious nodes are identified by the validation process. An IDS for the localization and detection of the anomalies in WSN is presented by[22]. The decision about the adversary is achieved by taking inference from the calculation and observation of the specially designated measurement nodes. Malicious node detection based on the neighbor node calculation is carried out in[23 24 25]. In[23], information fabrication attack is detected. Spatial correlation is used in order to detect anomalous activity in neighboring nodes. In[24], statistical distribution and high computational complexity of the nodes are the disadvantages of IDS. In[25] though, the cooperation between nodes makes this IDS robust, the main drawback is overhead due to communication. WSN requires a flexible, light weight and an effective IDS for the identification of internal malicious nodes. Therefore, a lightweight IDS is required. We present in this paper, a lightweight neighbor node trust calculation and evaluation based anomaly intrusion detection technique.

3. The proposed IDS

Block diagram of proposed intrusion detection system is shown in figure 1. The proposed intrusion detection system has a trust manager, which manage the direct and indirect trust (reputation) of a node. The behavior classifier classifies the behavior of the node as attacker, trustworthy and risky based on the trust values and calculation obtained from the trust manager. In case of the trustworthy behavior, the observed node is recommended to the forwarding engine for packet forwarding. When behavior of the observed node is identified as risky, its risk factor is evaluated and updated. If the observing node is willing to take risk, it recommends the observed node having risky behavior to the forwarding engine for forwarding. This status of the observed node is saved in the recommendation data base. If the observing node does not want to take risk, it stores the risk factor of the observed node in recommendation data base. In case of attack behavior, the attack classifier distinguishes attack pattern based on the calculation described in the following subsections. The observed node is declined for forwarding purpose. The status of the observed nodes is saved in the recommendation data base.

3.1. System Model and nodes Initial Observation

In the proposed IDS, a node y_0 calculates the level of trust of its neighboring nodes. The neighbors of y_0 is a set of nodes having one hop contact with node y_0 and are represented as $N_b(y_0)$=$\{y_1.....y_n\}$. Any node y_i possesses set of attributes denoted as $A_{y_i} = \{a_1.....a_n\}$. The activity of the node y_i is observed by the sensor node y_0 by observing its individual attributes. The observed attributes of node y_i are stored by the vector fy_i=$\{f_1y_i.....f_sy_i\}$ with every element explaining the node's activities in one feature. If node y_i observes its neighboring nodes $N_b(y_0)$=$\{y_1.....y_n\}$, it stores

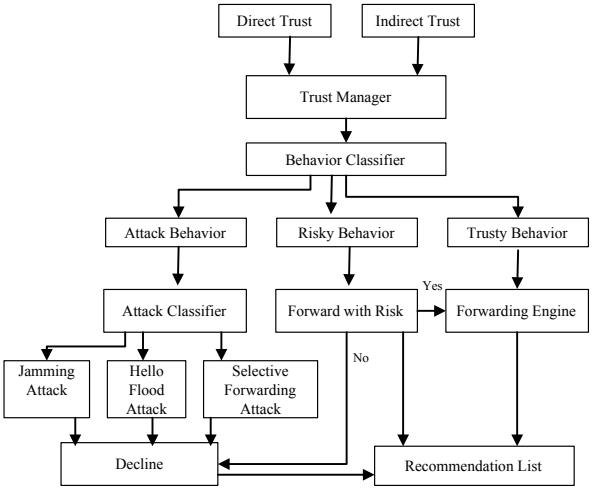

Fig. 1. Block Diagram of Proposed IDS

the set of the corresponding attribute vectors $A_{N_b(y_0)} = \{A_{y_1}.....A_{y_n}\}$. More precisely the attributes of any node include Received Signal Strength, Packet Sending Rate, Control Packet Generating Rate, Packets Delivery Ratio, Packet Dropping Rate, Packet Forwarding Rate and Packet Acknowledgment Rate. The amount of power in any radio signal received is termed as Received Signal Strength. The Received Signal Strength of the node y observed by the node y_0 is represented as $P_s(y)$. A node is considered malicious if it has high received signal strength than the vector of received signal strength of its neighbors $N_b(y_0)$=$\{y_1.....y_n\}$. In this case the node is considered to have undergone a Jamming attack. Packet Generation Rate is the number of control packets generated in a specific interval of time. $P_g(y)$ is the Packet Generation Rate of node y monitored by the node y_0. A node is considered malicious if it generates high number of control packets than the vector of control packets generated by its neighbors $N_b(y_0)$=$\{y_1.....y_n\}$. In this case, the node is considered to have undergone a Hello Flood attack. Packet Receiving Rate is the total number of packets received in a specific period of time. $PR_cR(y)$ is the Packet Receiving Rate of node y monitored by the node y_0. In a multi-hop scenario, a node forwards packets of its neighbors. The rate of packet received by a node and its subsequent forwarding to its destination node is termed as Packet Forwarding Rate. $PF_rR(y)$ is the Packet Forwarding Rate of node y monitored by the node y_0. A node is said to be suffering selective forwarding attack if its packets forwarding rate is much less than the packets forwarding rate of its neighbor $N_b(y_0)$=$\{y_1.....y_n\}$. Node's trust level is calculated based on these attributes. There are three possibilities about the observed node i.e. a node may be trustworthy or it may be a malicious or a risky node. These three kind of observations are saved in the recommendation data base of the IDS. Trust is calculated by taking average of the direct trust A(y) and indirect trust i.e reputation B(y). Mathematically $T(y) = avg[A(y), B(y)]$. The average of normal expected behavior of the neighboring nodes (T) is the required Trust (RT).

3.2. Detection of Jamming Attack

Let $P_{s0}(y)$ is the total Received Signal Strength of node y observed by node y_0 during time interval T_0. $P_{s1}(y)$ is the total Received Signal Strength of node y observed by node y_0 during time interval T_1 and $P_{sz}(y)$ is the total packet sending rate of node y observed by node y_0 during time interval T_z. let $P_{si}(y)$) is the total Received Signal Strength of node y observed by node y_0 during time interval T_i. Then the average Received Signal Strength is calculated as $P_{savg}(y) = \sum_{t=1}^{z}(t/z)[P_{st}(y)]$. Now at any interval '$i$' if the Received Signal Strength is greater then the summation of average Received Signal Strength and the Received Signal Strength values of the sensor specified in its data sheets, node is suffering from jamming Attack. Mathematically,

$$P_{si}(y) > P_{savg}(y) + C \tag{1}$$

Where $P_{si}(y)$ is the Received Signal Strength of node y at any given interval i observed by node y_0. C is the Received Signal Strength values of the sensor specified in its data sheets. Node for which equation 1 does not not hold true, are malicious.

3.3. Detection of Selective Forwarding Attack

The packets forwarded successfully is the ratio in between the packet forwarding rate $PF_rR(y)$ and packet receiving rate $PR_cR(y)$. The packets forwarded successfully by node y at any instant 'i' observed by node y_0 is given as $P_{f_i}(y) = \frac{PF_rR(y)}{PR_cR(y)}$.

Let $P_{f_i}(y)$ is the total packets forwarded successfully by node y observed by node y_0 during time interval T_0. $P_{f1}(y)$ is the total packets forwarded successfully by node y observed by node y_0 during time interval T_1 and $P_{f_z}(y)$ is the total packets forwarded successfully by node y observed by node y_0 during time interval T_z. let $P_{f_i}(y)$ is the total packets forwarded successfully by node y observed by node y_0 during time interval T_i. Then the average packets forwarded successfully is calculated as $P_{f_{avg}}(y) = \sum_{t=1}^{z}(t/z)[P_{f_t}(y)]$. Now at any interval '$i$' if the packets forwarded successfully is greater then the summation of average of packets forwarded successfully, node is suffering from jamming Attack. Mathematically,

$$P_{f_i}(y) > P_{f_{avg}}(y) \tag{2}$$

Where $P_{f_i}(y)$, in the above equation is the packets forwarded successfully by node y at any instant i observed by node y_0. $PF_rR(y)$ is the packet forwarding rate of the node y and $PR_cR(y)$ is the packet receiving rate of node y at any particular interval. We can say that node for which equation 2 does not not hold true, are malicious.

3.4. Detection of HELLO Flood Attack

Let $P_{g0}(y)$ is the control packets generating rate of node y observed by node y_0 during time interval T_0. $P_{g1}(y)$ is the packets generating rate of node y observed by node y_0 during time interval T_1 and $P_{g_z}(y)$ is the control packets generating rate of node y observed by node y_0 during time interval T_z. Let $P_{g_i}(y)$) is the control packets generating rate of node y observed by node y_0 during time interval T_i. Then the average control packets generating rate is given as $P_{g_{avg}}(y) = \sum_{t=1}^{z}(t/z)[P_{g_t}(y)]$. Now at any interval '$i$' if the control packets generating rate of any node is greater then the summation of average control packets generating rate and the control packets generating rate values of the sensor specified in the standard protocol, node is suffering from Hello Flood Attack. Mathematically

$$P_{g_i}(y) > P_{g_{avg}}(y) + C \tag{3}$$

Where $P_{g_i}(y)$ is the control packets generating rate of node y at any given interval i observed by node y_0 . C is the control packets generating rate values of the sensor specified in the standard protocol it follow. Node for which equation 3 does not hold true, are malicious and higher control packets generating rate is the identification of hello flood attack.

3.5. Detection of Trustworthy (Good) Nodes

A node is said to be trustworthy or Good if its current Direct Trust value $A_c(y)$ is greater or equal to the required trust value RT_v , meaning that it satisfies the condition $A_c(y) \geq RT_v$.

3.6. Detection of Risky Nodes

There are two possibilities about the risky nature of a node. In the first case, there is no prior recommendation about the node , that is $B(y)$=0 and its current direct trust value $A_c(y)$ is less that the Required Trust Value RT_v. Mathematically: $A_c(y) < RT_v$. In this case, the total trust is given as $T_{TA}(y) = A_c(y) + B(y)$ and as $B(y)$=0 so $T_{TA}(y) = A_c(y)$. Then the value of risk is given as $R_A(y) = RT_v - T_{TA}(y)$

$$R_A(y) = RT_v - T_{TA}(y) \tag{4}$$

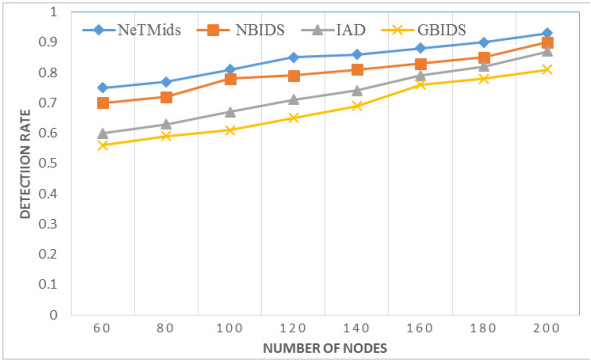

Fig. 2. Detection rate per 100 rounds along varying network size

In the second case, the recommendation value of the node is less than the value of Required Trust Value that is $B(y) < RT_v$ and its current direct trust value $A_c(y)$ is less that the Required Trust Value RT_v. Mathematically $A_c(y) < RT_v$. In this case, the total trust is given as $T_{TB}(y) = A_c(y) + B(y)$. Then the value of risk is given by the following equation.

$$R_B(y) = RT_v - T_{TB}(y) \tag{5}$$

3.7. Storage of Node Status for future use (Reputation) and subsequent Forwarding Decision

Recommendation Data Base stores the status of the node. On the bases of calculation, a node may be found malicious, trustworthy or risky. These statistics are used in the future interaction of the nodes. A trustworthy node is recommended for interaction, a malicious node is declined, while decision about packet forwarding through risky node is mad, if the node intending to send data is willing to take risk. After the successful determination of the node status as malicious, trustworthy or risky, decision about the packet forwarding through any neighbor node is taken by the packet sending node. The criteria for packet forwarding is the selection of safest path rather than selecting shortest path.

4. Results and Discussion

The proposed intrusion detection system is implemented using MATLAB. Nodes were randomly deployed in an area of 200 x 200 square meters. Simulations were performed for network size of 60, 80, 100, 120,140, 160, 180, and 200 nodes. For each network size, per 100 round results are discussed for the detection rate of the proposed IDS. The detection rate of the proposed IDS is compared with the detection rate of[23],[24] and[25]. Figure 2 shows that the average detection rate of the proposed NeTMids is 0.8 which is better than the detection rate of[23],[24] and[25], due to the fact that the proposed IDS distinguishes observed nodes as trustworthy, risky and malicious based on their trust values. Also observing node does not solely depend on the observed node reputation but it also takes into consideration the calculated values of its current trust.

5. Conclusion

We propose an intrusion detection technique based on the principal that nodes in each other neighborhood behave in a similar way. The proposed NeTMids detects hello flood, jamming and selective forwarding attack. It can be further extended by including other attacks as well. Simulation results shows that network perform better when the proposed NeTMids is deployed.

References

1. C. Chong and S. Kumar "Sensor networks: Evolution, opportunities, and challenges", *Proc. IEEE,* vol. 91, no. 8, pp.1247 -1256 2003.
2. C. Karlof and D. Wagner, "Secure Routing in Wireless Sensor Networks: Attacks and Countermeasures", *Ad Hoc Networks,* vol. 1, pp.293 -315 2003.
3. Martins, D.; Guyennet, H., "Wireless Sensor Network Attacks and Security Mechanisms: A Short Survey," *Network-Based Information Systems (NBiS), 2010 13th International Conference on* , vol., no., pp.313,320, 14-16 Sept. 2010.
4. K Xing, S Srinivasan, M Rivera, J Li, X Cheng, ed. by SCH Huang, D MacCallum, and D-Z Du, Attacks and countermeasures in sensor networks: A survey, *in Network Security* , pp. 251-272, Springer, New York, 2010.
5. I. Krontiris, T. Dimitriou, and F. C. Freling, "Towards intrusion detection in wireless sensor networks," *in EW 2007: Proceeding of the 13th Eurpoean Wireless ConferenceL Enabling Technologies for Wireless Multimedia Communications*, April 2007.
6. A. Farooqi and F. Khan, "Intrusion detection systems for wireless sensor networks: A survey," *Communication and Networking,* pp. 234-241, 2009.
7. Z. S. Bojkovic, B. M. Bakmaz and M. R. Bakmaz, "Security issues in wireless sensor networks", *International Journal of Communications,* vol. 2, no. 1, 2008.
8. M.Momani,, "Bayesian Methods for Modeling and management of Trust in Wireless Sensor Networks", *PhD Thesis, Faculty of Engineering, University of Technology*, Sydney July, 2008.
9. F. Azziden and M. Maheshwaran, "Evolving and Managing Trust in Grid Computing", *in IEEE Canadian Conference on Electrical and Computer Engineering (CCECE '02),* 2002.
10. S.D. Kamvar, M.T. Schlosser, H. GarciaMolina, "The Eigen trust algorithm for reputation management in P2P networks", *in: Proceedings of the 12th International Conference on World Wide Web,* pp. 640-651, 2003.
11. X. Chen, K. Makki, K. Yen, N. Pissinou, "Sensor network security: A survey", *IEEE Communications Surveys and Tutorials*, vol. 11, no. 2, pp. 52-73, June 2009.
12. Feng, R., X. Xu, X. Zhou and J. Wan, "A trust evaluation algorithm for wireless sensor networks based on node behaviors and d-s evidence theory," *Sensors, 11:*,pp. 1345-1360, 2011.
13. H. Deng, Y. Yang, G. Jin, R. Xu, W. Shi, "Building a trust-aware dynamic routing solution for wireless sensor networks," *in: IEEE Globecom 2010 Workshop on Heterogeneous, Multi-Hop Wireless and Mobile Networks,* pp.153157, 2010.
14. Poolsappasit, N.; Madria, S.K., "A Secure Data Aggregation Based Trust Management Approach for Dealing with Untrustworthy Motes in Sensor Network," *Parallel Processing (ICPP), 2011 International Conference on* , vol., no., pp.138,147, 13-16 Sept. 2011.
15. Furong Wang; Huang Chen; Jing Zhao; Chunming Rong, "IDMTM: A Novel Intrusion Detection Mechanism Based on Trust Model for Ad Hoc Networks," *Advanced Information Networking and Applications, 2008. AINA 2008. 22nd International Conference on* , vol., no., pp.978,984, 25-28 March 2008.
16. Ebinger, P.; Bissmeyer, N., "TEREC: Trust Evaluation and Reputation Exchange for Cooperative Intrusion Detection in MANETs," *Communication Networks and Services Research Conference, 2009. CNSR '09. Seventh Annual,* vol., no., pp.378,385, 11-13 May 2009.
17. S. Ganeriwal, L.K. Balzano, and M.B. Srivastava, "Reputation-based framework for high integrity sensor networks," *ACM Transitions on Sensor Network,* vol. 4, no. 3, May 2008.
18. K. Liu, N. Abu-Ghazaleh, and K.-D. Kang, "Location verification and trust management for resilient geographic routing," *J. Parallel and Distributed Computing,* vol. 67, no. 2, pp. 215-28, 2007.
19. R.A. Shaikh, H. Jameel, B.J. dAuriol, H. Lee, S. Lee, and Y.J. Song, "Group-based trust management scheme for clustered wireless sensor networks," *IEEE Transactions on Parallel and Distributed Systems,* vol. 20, no. 11, pp. 1698-1712, Nov. 2009.
20. Fenye Bao; Ing-Ray Chen; MoonJeong Chang; Jin-Hee Cho, "Trust-Based Intrusion Detection in Wireless Sensor Networks," *Communications (ICC), 2011 IEEE International Conference on,* vol., no., pp.1,6, 5-9 June 2011.
21. Renyong Wu; Xue Deng; Rongxing Lu; Xuemin Shen, "Trust-based anomaly detection in wireless sensor networks," *Communications in China (ICCC), 2012 1st IEEE International Conference on,* vol., no., pp.203,207, 15-17 Aug. 2012.
22. S. Zheng and J. Baras, "Trust-assisted anomaly detection and localization in wireless sensor networks," *in Proc. IEEE Conf. on Sensor, Mesh and Ad Hoc Comm. and Netw (SECON),* pp. 386394, 2011.
23. A. Stetsko, L. Folkman, and V. Matyayas, "Neighbor-Based Intrusion Detection for Wireless Sensor Networks," *in International Conference on Wireless and Mobile Communications Los Alamitos, CA, USA,* pp. 420-425, 2010.
24. F. Liu, X. Cheng, and D. Chen, "Insider attacker detection in wireless sensor networks," *in Proceedings of IEEE INFOCOM,* pp. 1937-1945, 2007.
25. G. Li, J. He, and Y. Fu, "A group-based intrusion detection scheme in wireless sensor networks," *in Proceedings of GPS - Workshops,* pp. 286-291, IEEE, 2008.
26. Xu,W., Trappe,W., Zhang, Y. and Wood, T. "The feasibility of launching and detecting jamming attacks in wireless networks", *In MobiHoc 05: Proceedings of the 6th ACM international symposium on Mobile ad hoc networking and computing,* New York, USA, ACM 4657, 2005.
27. Wenyuan Xu; Ke Ma; Trappe, W.; Zhang, Y., "Jamming sensor networks: attack and defense strategies," *Network, IEEE* , vol.20, no.3, pp.41,47, May-June 2006.