A Novel Energy-Efficient Sybil Node Detection Algorithm for Intrusion Detection System in Wireless Sensor Networks

A. Babu Karuppiah, J. Dalfiah, K. Yuvashri
Velammal College of Engineering & Technology,
Madurai-625009, India
babu_karuppiah@yahoo.co.in

S. Rajaram
Thiagarajar College of Engineering,
Madurai-625015, India
rajaram_siva@tce.edu

Al-Sakib Khan Pathan
Department of Computer Science,
International Islamic University Malaysia,
Kuala Lumpur, Malaysia
sakib@iium.edu.my

***Abstract*— A Wireless Sensor Network (WSN) is vulnerable to different types of security attacks where the attackers could easily intrude into the network and could cause inexplicable destruction by disrupting the expected functionalities of the network. Severe drainage of battery may occur due to the attacks and as a result, the lifetime of the network may decrease drastically. In this paper, an energy-efficient integrated Intrusion Detection System (IDS) is proposed to detect network layer Sybil attack. Our scheme spots out accurately and purges out the Sybil node which may falsely behave as a genuine node. The experimental results show that the critical factor in WSN, energy is conserved more efficiently by the proposed scheme than the existing alternative methods. Also, accurate detection of the malicious node is possible spending relatively less energy.**

Keywords- Attacks; Efficient; Energy; Integrated; Intrusion; Sybil; Network; Security; Sensor; Wireless

I. INTRODUCTION

Majority of the networks depend on the supposition of identity, where each participating entity holds a single identity. Trouble occurs when a reputation system is deceived into believing that an attacker has disproportionately higher authority. Likewise, an attacker with multiple identities can utilize them to operate maliciously, by either embezzling data or disrupting communication between nodes. Such an attack is called Sybil attack that threatens the reputation system of a peer-to-peer kind of network by launching a huge number of pseudonymous identities which are used for exercising undue authority in the network. Thus, in the Sybil attack, by imitating other nodes in the network or merely by claiming fake identities, a malicious node conducts itself as if it were a larger number of nodes. A Sybil attacker may also create a random number of supplementary node identities, using only a single physical device [1].

A reputation system's weakness to a Sybil attack depends on how cheaply identities can be generated, the level to which the system of reputation agrees to get inputs from the nodes that lack a chain of mutual trust connecting them to a trusted entity, and whether the system of reputation cares for all entities identically.

A section of software that has access to local resources is known as an entity on a peer-to-peer network. The objective of an entity is to advertise itself on the network by offering an identity. Multiple identities can relate to a single entity. The purposes of entities using multiple identities are redundancy, resource sharing, reliability, and integrity. In peer-to-peer networks, utilization of the identity is in the form abstraction, thus a remote entity becomes conscious of other identities without essentially knowing the association of identities to local entities. By default, each unique identity is normally assumed to correspond to a unique local entity. In reality, multiple identities may get associated to the same local entity. The sensors in a WSN often communicate among themselves in a peer-to-peer fashion for which all the issues mentioned here are applicable to WSNs of this nature as well. Given this understanding, in this paper we devised a scheme to tackle the threat of Sybil attack.

II. RELATED WORKS

A few works that were published before motivated us to devise our mechanism. In this section, we note those briefly. A mechanism based on signal strength is proposed by the author of [2], which describes a method of detecting malicious adversaries in a network. The idea is to compare the signal strengths from the reception side with its expected value. The vulnerabilities of the trust mechanism are addressed in [3] where the authors discuss the various weaknesses of the stages of trust mechanism. They propose a Watchdog monitoring system by adding together a threshold mechanism. This mechanism requires more time to make a decision compared to a network without a tolerance threshold. The authors of [4] propose an extended Watchdog mechanism for WSN.

The work proposed by [5] uses a monitoring neighbor that warns the sending node and the Base Station (BS) when an insider launches an attack by dropping packets. The constraint of this method is better understood when neighbor nodes accuse good nodes falsely as malicious nodes. Moreover, it cannot address selective forwarding issue [6]. The authors of [7] have proposed a methodology for detecting selective forwarding attacks. Here, relative communication overhead seems to be higher in terms of number of compromised nodes. The authors of [8] have proposed an algorithm for detection, diagnosis, and isolation of nodes launching control attacks such as Wormhole, Sybil, Rushing, Sinkhole, and Replay attacks. An improved Watchdog monitoring system has been developed based on a power aware hierarchical model in [9]. The methodology solves the ambiguous Collision.

Some works have also gone to the direction of Sybil attack specifically. The method proposed by the authors of [1] is based on the resources used by a node. If a Sybil node exists, then it has to carry out the tasks of the identities it

978-1-4799-7002-5/14 $31.00 © 2014 IEEE
DOI 10.1109/Eco-friendly.2014.94

possess. Consequently, when it exceeds a threshold value, the Sybil node is detected. Recent works on Sybil defense mechanisms are based on Social network based schemes [10], [11], [12], [13], [14], [15]. Many defense schemes such as SybilGuard [16], SybilLimit [17], SybilControl [18] and SybilInfer [19] are proposed by authors to detect Sybil nodes.

III. Problem Formulation

Sybil attack can be used to attack numerous kinds of protocols in WSNs. Sybil threat can cause too much harm to WSN in routing, voting system, fair resource allocation, aggregation of data, and misbehavior detection. The Sybil attack in a distributed hash table, such as Geographic Hash Table (GHT), could very easily defeat replication and fragmentation [20]. From the literature survey, it is understood that one malicious Sybil node might be capable to play a role in the aggregation of the reading many times. With sufficient number of Sybil nodes, an adversary might entirely alter the aggregated reading. Moreover, the Sybil attacker stuffs the ballot box during voting process used in some WSNs. The Sybil attack can also be used to permit an adversary node to get hold of an unfair share of any resource. This declines service to be given to the legitimate nodes by bringing down their expected share of the resources, and gives the attacker more resources to carry out other attacks. Any misbehavior detector that can potentially spot out a specific type of misbehavior is likely to have some false positives. As a consequence, it might fail to take action until it detects numerous repetitive offenses by the same node. An attack with several Sybil nodes could spread the blame by not possessing any of the accused identities and thus, can cause complete chaotic situation in a network. So, an efficient mechanism has to be devised to detect the Sybil node and reduce the false positives while detecting the same.

IV. Proposed Scheme and Performance Evaluation

From the literature review, it is understood that an algorithm is required to detect Sybil node as well as to conserve energy during the process. While many other wireless networks may successfully use many existing solutions, for WSN, this is imperative to save energy alongside the efficiency of the mechanism. With this motivation, we propose here a unique algorithm. A major constraint in constructing a WSN is to improve the network life time. Nodes in a WSN are usually highly energy starved and they are expected to function for longer periods. Prediction of the lifetime of the sensor network accurately requires an accurate energy consumption model. In this work, a comprehensive energy model is adopted that includes sensing, logging, and switching energies apart from the processing and communication energy values [21]. Moreover, the overhearing energy is calculated from the work proposed in [22].

Let us take into account a WSN with a Cluster Head (CH) and a few numbers of nodes under it. The scenario considered (a single cluster) consists of four legitimate nodes, a CH, and a Sybil node. The same cluster structure would appear all over the network to cover up the entire Area of Interest (AoI). The network assumed has static nodes and the channel is noise-free during transmission. It is also assumed that the sensor motes have the same transmission power.

The cases considered for detection of Sybil nodes are:

Case 1: *A Sybil node does not reply to the query sent by the CH.* For finding out the solution for Case 1, the proposed algorithm is implemented with a centralized approach. It is based on sending and acknowledging the query data packets. The CH preserves a table that comprises of the identities of each node against its location information. The pair remains to be unique for a specific node. Figure 1 in the form of the flow chart shows the procedure to detect the Sybil nodes using the proposed algorithm.

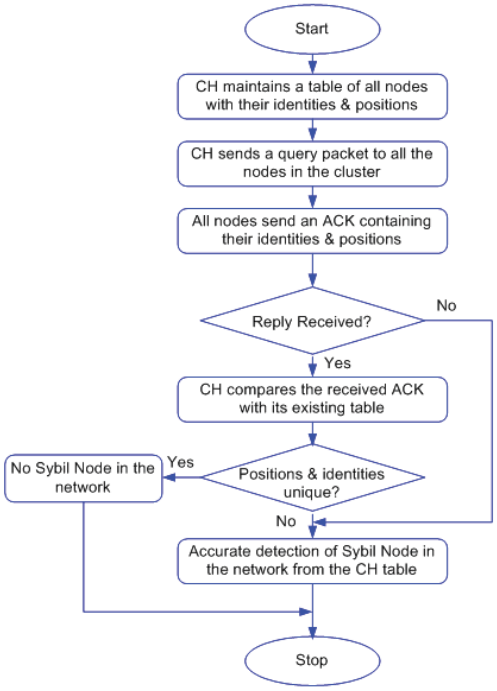

Figure 1. Proposed algorithm – SybilSecure.

Case 2: *Sybil node replies with same identity and different coordinates.* In this scenario, all the genuine nodes answer to the CH with their identities and location coordinates. The Sybil node also provides a response to the CH with any one of the nodes' identities and its own locality. For instance, if a CH in its coverage range has 4 nodes say, x_1, x_2, x_3, x_4 with the locations L_1,L_2,L_3,L_4 respectively, Sybil node must have any one these identities (x_1, x_2, x_3, x_4) and its own location x_5. If the Sybil node responds with any one of these identities and the location x_5, as the CH already has the set of legitimate nodes' identities with their location coordinates in its table, it would be easily identified as the Sybil node (as there would be conflict in the claim and the information that is preserved in the table).

Existing Watchdog mechanism has the limitation of not being able to detect the misbehaving nodes which upsets the routing of packets in the network. Our objective is to improvise the monitoring of malicious nodes that leads to energy-efficient operation and accurate detection of malicious nodes.

The sink of the WSN receives packets when the nodes respond to it in the routing path. It then analyzes for the malicious nodes. The sink gathers the status bits in subsequent packet transmissions as noted in Algorithm 1.

ALGORITHM 1

Let S_0 – Source node ; S_i, S_{i+1}, …… S_n – Input node ; S_k – Sink node; S_{mi} - Malicious node

1. **for** each S_i watches S_{i+1} whether data sent successfully or not
2. At the same time S_0 sends the data to S_i
3. **if** S_{i+1} is a true node
4. response bit of S_i is zero
5. **else**
6. response bit of S_i can send zero or one
7. **end if**
8. **end for**
9. When it reaches S_n all the response bit will be sent to S_k
10. By fixing the suspicious point, the exact S_{mi} will be found out.

It is considered that the positions of the sensor nodes remain unaltered and also have the same transmission power except for the malicious node as it is able to alter its power of transmission. The sensor nodes are considered to only sense data and transmit to their neighbors during each and every round. The dissipation of energy due to processing of data from regular sensor nodes is neglected. The sensor energy model of [23] is considered and the parameters are considered accordingly. The algorithm was evaluated in C++ and simulation results were acquired for the WSN. In the simulations, a WSN with the number of nodes, Ns = 4 was considered initially and the number was increased later on. The deployment of the motes is random within the square 400m × 400m is considered. The deployed sensor nodes are homogeneous; therefore, consumption of energy for all behaviors except the communication energy due to diverse transmission distances to the BS, should be alike for each and every sensor node.

Case 1 that has been mentioned earlier, where the Sybil node does not reply to the CH after a query packet is sent is solved by the proposed improved watchdog monitoring mechanism. The identification of malicious nodes in a network is shown in Figure 2 for both the existing Watchdog mechanism and the proposed algorithm. The graph is plotted for the number of rounds against the nodes.

It is inferred that the watchdog monitoring mechanism taken as reference, portrays a different node in each round to be an adversary node and to detect the precise malicious node, it expends additional rounds and as a result more energy is consumed in the monitoring process.

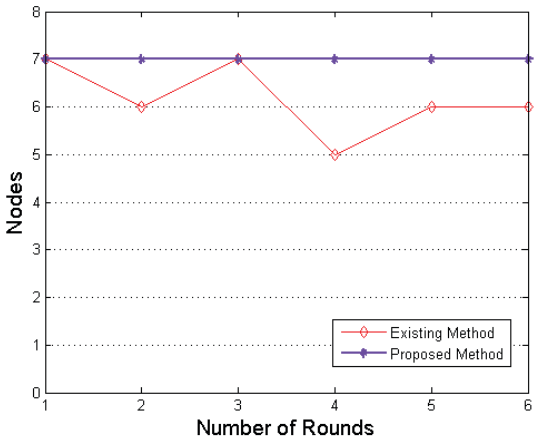

Figure 2. Identification of exact malicious nodes.

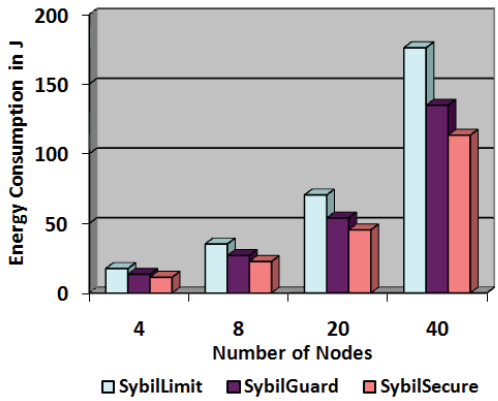

Figure 3. Number of nodes vs Energy consumption.

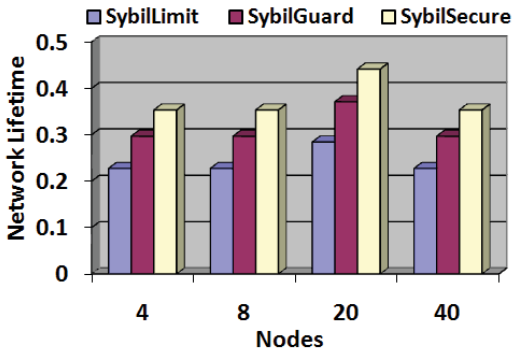

Figure 4. Number of nodes vs Network lifetime.

SybilSecure, the proposed algorithm aims at solving the Case 2 where the Sybil node takes on multiple identities and replies with different location details. From the obtained results, it can be understood that the energy consumed by the proposed algorithm to detect Sybil attack consumes lesser energy than that of the existing methods.

Figure 3 shows the simulation results of existing techniques compared with the proposed method. SybilSecure spends about 11.327 J to determine a Sybil node accurately. But the other recent social network based defense practices such as SybilGuard and SybilLimit consume additional energy than SybilSecure. SybilGuard utilizes around 8.8 J for a period of time which will become worse when it runs for longer period. SybilLimit consumes about 13.48 J for a single round.

Figure 4 shows that the network lifetime is enhanced when the proposed technique is applied to determine the Sybil node in the network.

V. Discussion and Conclusions

An integrated Intrusion Detection System (IDS) is proposed especially to detect a Sybil node and misbehaving malicious node. It becomes mandatory to detect these adversaries to prevent the network from loss or tampering of packets. Optimization in energy in the case of WSN is much more intricate than conventional low-power design techniques because it engages in not only reducing the consumption of energy of a single sensor node but also in increasing the lifetime of an entire network. This work has taken both the criteria of detecting the adversary node accurately and enhancing the lifetime of the network into consideration. The proposed system implemented eliminates the greatest limitation of the existing Watchdog mechanism, the false detection of malicious node (i.e., false positives). The simulation results and analysis show that the algorithm proposed for detecting Sybil nodes improves the energy-efficiency than the prevailing watchdog monitoring system. Also, it is found that the technique proposed detects the illegitimate node accurately whereas the existing method fails to identify it accurately. The reduction in energy consumption for the network-setup bears out to be very significant for WSN. The proposed approach comes very handy even with densely deployed networks. In this work, detecting the presence of a single malicious node in the network is basically focused. The idea could also assist in detecting colluding nodes in the network.

References

[1] J. Newsome, E. Shi, D. Song, and A. Perrig, "The Sybil Attack in Sensor Networks: Analysis & Defenses," Third International Symposium onInformation Processing in Sensor Networks, 2004. IPSN 2004, pp. 259–268, 26-27 April 2004.

[2] V. Varadharajan, "A Note on Trust-Enhanced Security," IEEE Security & Privacy, Vol. 7, Issue. 3, pp. 57-59, 2009.

[3] Y. Cho, G. Qu, and Y. Wu, "Insider Threats against Trust Mechanism with Watchdog and Defending Approaches in Wireless Sensor Networks," in Proc. of IEEE Symposium on Security and Privacy Workshops, pp. 134-141. , 24-25 May 2012.

[4] L. Huang and L. Liu, "Extended Watchdog Mechanism for Wireless Sensor Networks," Journal of Information and Computing Science, Vol.3, No. 1, pp. 39-48, 2008.

[5] W. Xin-sheng, Z. Yong-zhao, X. Shu-ming, and W. Liang-min, "Lightweight Defense Scheme Against Selective Forwarding Attacks in Wireless Sensor Networks," International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery, 2009 (CyberC'09), pp. 226-232, 10-11 Oct. 2009.

[6] A.-S.K. Pathan, W. M. Abduallah, S. Khanam, and H. Y. Saleem, "A Pay-and-Stay Model for Tackling Intruders in Hybrid Wireless Mesh Networks," SIMULATION: Transactions of The Society for Modeling and Simulation International, Volume 89, Issue 5, pp. 616-633, May 2013.

[7] B. Xiao, B. Yu, and C. Gao, "CHEMAS: Identify Suspect Nodes in Selective Forwarding Attacks," Journal of Parallel and Distributed Computing, Volume 67, Issue 11, pp. 1218–1230, November 2007.

[8] I. Khalil, S. Bagchi, C. N. Rotaru, and N. B. Shroff, "UnMask: Utilizing Neighbor Monitoring for Attack Mitigation in Multihop Wireless Sensor Networks," Ad Hoc Networks, Volume 8, Issue 2, pp. 148-164, March 2010.

[9] A. Forootaninia and M. B. Ghaznavi-Ghoushchi, "An Improved Watchdog Technique based on Power-Aware Hierarchical Design for IDS In Wireless Sensor Networks," International Journal of Network Security & Its Applications, Vol. 4, Issue 4, p. 161, July 2012.

[10] J. R. Douceur, "The Sybil Attack," Proc. of 1st Int. Workshop on Peer-to-Peer Systems, LNCS, vol. 2429. Cambridge, MA, USA: Springer, pp. 251-260, 2002.

[11] B. N. Levine, C. Shields, and B. N. Margolin, A Survey of Solutions to the Sybil Attack. University of Massachusetts Amherst, Amherst, MA, Technical Report, 2006, available at: https://gnunet.org/node/1432 [last accessed: 17 May 2014]

[12] B. Viswanath, M. Mondal, A. Clement, P. Druschel, K. P. Gummadi, A. Mislove, and A. Post, "Exploring the Design Space of Social Network-Based Sybil defenses," Fourth International Conference on Communication Systems and Networks (COMSNETS), 2012, pp. 1-8, 3-7 Jan. 2012.

[13] N. Tran, J. Li, L. Subramanian, and S. S. M. Chow, "Optimal Sybil-Resilient Node Admission Control," Proc. of IEEE INFOCOM, pp. 3218-3226, 10-15 April 2011.

[14] B. Viswanath, A. Post, K. P. Gummadi, and A. Mislove, "An Analysis of Social Network-Based Sybil Defenses," ACM SIGCOMM Computer Communication Review - SIGCOMM '10, Volume 40 Issue 4, pp. 363-374,October 2010.

[15] N. Balachandran and S. Sanyal, "A Review of Techniques to Mitigate Sybil Attacks," International Journal of Advanced Networking & Applications, Vol. 4 Issue 1, p. 1514, Jul/Aug2012.

[16] H. Yu, M. Kaminsky, P. B. Gibbons, and A. Flaxman, "SybilGuard: Defending Against Sybil Attacks via Social Networks," IEEE/ACM Transactions on Networking, Vol. 16, No. 3, pp. 576-589, June 2008.

[17] H. Yu, M. Kaminsky, P. B. Gibbons, and F. Xiao, "SybilLimit: A Near-Optimal Social Network Defense against Sybil Attacks," IEEE/ACM Transactions on Networking, Vol. 18, No. 3, pp. 885 – 898, June 2010.

[18] F. Li, P. Mittal, M. Caesar, and N. Borisov, "SybilControl: Practical Sybil Defense with Computational Puzzles," Proceedings of the seventh ACM workshop on Scalable trusted computing (STC 2012), pp. 67-78, 2012.

[19] G. Danezis and P. Mittal, "SybilInfer: Detecting Sybil Nodes Using Social Networks," Proc. of ISOC NDSS, February 2009.

[20] S. Ratnasamy, B. Karp, L.Yin, D. Estrin, R. Govindan & S. Shenker, 2002, 'GHT: A geographic hashtable for data-centric storage', Proceedings of WSNA, pp. 78-87.

[21] N. Halgamuge, M. Zukerman, K. Ramamohanarao, and H. L. Vu, "An Estimation of Sensor Energy Consumption," Progress in Electromagnetics Research B, Vol. 12, pp. 259–295, 2009.

[22] P. Basu and J. Redi, "Effect of Overhearing Transmissions on Energy Efficiency in Dense Sensor Networks," Proc. of 3rd Int. Symposium on Information Processing in Sensor Networks, pp. 196-204, 26-27 April 2004.

[23] R. Jurdak, A. G. Ruzzelli, and G. M. P. O'Hare, "Radio Sleep Mode Optimization In Wireless Sensor Networks," IEEE Transactions on Mobile Computing, Vol. 9, No. 7, pp. 955–968, July 2010.