INTERNATIONAL JOURNAL OF ADVANCED RESEARCH IN COMPUTER SCIENCE AND ENGINEERING TECHNOLOGIES

ISSN 2454-9924 Volume: 1 Issue: 1(2015)

Detection of Look Alike Detection of Clone Node and Collusion Attacks in WSN

R. Aswini #1, P. R. Jayanthi *1

Mailam Enginnering College, Mailam #1, *1

Raswini29@gmail.com #1

Abstract - The combination of node is naturally accomplished due to computational power and energy resources. In the previous mechanism, Wireless sensor networks are vulnerable to the node clone, and several distributed protocols have been proposed to detect this attack. So they require too strong assumptions to be practical for large-scale, randomly deployed sensor networks. In the proposed mechanism, we use two new node clone detection protocols with different agreement on network conditions and performance. The first one is based on a Distributed Hash Table (DHT) in which Chord algorithm is used to detect the cloned node, every node is assigned with the primary key, and before it transfer the data it has to give its key which would be verified by the proof node. If same key is given by another Node then the proof node detects the cloned Node. The second one is based on the Distributed Detection Protocol which is same as DHT, but it is easy and cheaper determination. Here every node only needs to know the neighbor-list containing all neighbor IDs and its locations. In the modified Process, we are determining RDE protocol, by location based nodes detection, where every region/location will have a group leader. The Group leader will generate a random number with time stamp to the available nodes in that location. Witness nodes verify the random number and time stamp to detect the cloned node. Here, it also provides security measures.

Key Words – Computational Power, Energy resources, Distributed Hash Table, Time Stamp

1 Introduction

DUE to a need for robustness of monitoring and low cost of the nodes, wireless sensor networks (WSNs) are usually redundant. Data from multiple sensors is aggregated at an aggregator node which then forwards to the base station only the aggregate values. At present, due to limitations of the

Copyright © 2015 IJARCSET. All rights reserved.

INTERNATIONAL JOURNAL OF ADVANCED RESEARCH IN COMPUTER SCIENCE AND ENGINEERING TECHNOLOGIES

ISSN 2454-9924 Volume: 1 Issue: 1(2015)

computing power and energy resource of sensor nodes, data is aggregated by extremely simple algorithms such as averaging. However, such aggregation is known to be very vulnerable to faults, and more importantly, malicious attacks. This cannot be remedied by cryptographic methods, because the attackers generally gain complete access to information stored in the compromised nodes. For that reason data aggregation at the aggregator node has to be accompanied by an assessment of trustworthiness of data from individual sensor nodes. Thus, better, more sophisticated algorithms are needed for data aggregation in the future WSN. Such an algorithm should have two features. 1. In the presence of stochastic errors such algorithm should produce estimates which are close to the optimal ones in information theoretic sense. Thus, for example, if the noise present in each sensor is a Gaussian independently distributed noise with zero mean, then the estimate produced by such an algorithm should have a variance close to the Cramer- Rao lower bound (CRLB), i.e, it should be close to the variance of the Maximum Likelihood Estimator (MLE). However, such estimation should be achieved without supplying to the algorithm the variances of the sensors, unavailable in practice. 2. The algorithm should also be robust in the presence of non-stochastic errors, such as faults and malicious attacks, and, besides aggregating data; such algorithm should also provide an assessment of the reliability and trustworthiness of the data received from each sensor node. Trust and reputation systems have a significant role in supporting operation of a wide range of distributed systems, from wireless sensor networks and e-commerce infrastructure to social networks, by providing an assessment of trustworthiness of participants in such distributed systems. A trustworthiness assessment at any given moment represents an aggregate of the behavior of the participants up to that moment and has to be robust in the presence of various types of faults and malicious behavior. There are a number of incentives for attackers to manipulate the trust and reputation scores of participants in a distributed system, and such manipulation can severely impair the performance of such a system. The main target of malicious attackers is aggregation algorithms of trust and reputation systems.

2 Related work

In the previous mechanism, Wireless sensor networks are vulnerable to the node clone,

Copyright © 2015 IJARCSET. All rights reserved.

ISSN 2454-9924 Volume: 1 Issue: 1(2015)

and several distributed protocols have been proposed to detect this attack. So they require too strong assumptions to be practical for large-scale, randomly deployed sensor networks. Here it provides some, drawbacks are, Less Security, Data hacking, missing privacy

2.1 Proposed Mechanism

In the proposed mechanism, we use two novel node clone detection protocols with different tradeoffs on network conditions and performance. The first one is based on a distributed hash table (DHT) in which Chord algorithm is used to detect the cloned node, every node is assigned with the unique key, and before it transmits the data it has to give its key which would be verified by the witness node. If same key is given by another Node then the witness node identifies the cloned Node. The second one is based on the Distributed Detection Protocol which is same as DHT, but it is easy and cheaper implementation. Here every node only needs to know the neighbor-list containing all neighbor IDs and its locations. In the modified system, Process, we are implementing RDE protocol, by location based nodes identification, where every region/location will have a group leader. The Group leader will generate a random number with time stamp to the available nodes in that location. Witness nodes verify the random number and time stamp to detect the cloned node. The message is also encrypted for security purpose. Here, it provides some advantages are, High security, Data integrity, easily find the attacker

3 Methodologies

3.1 Establishment of Network

This module is developed in order to create a dynamic network. In a network, nodes are interconnected with the admin, which is monitoring all the other nodes. All nodes are sharing their information with each other's

3.2 Distribution of Proof node

A major issue in designing a protocol to detect clone attacks is the selection of the witnesses. We will call 'Witness' as a node that detects the existence of a node in two different locations within the same protocol run. If the adversary knows the future witnesses before the detection protocol executes, the adversary could subvert these nodes so that the attack goes undetected.

Copyright © 2015 IJARCSET. All rights reserved.

INTERNATIONAL JOURNAL OF ADVANCED RESEARCH IN COMPUTER SCIENCE AND ENGINEERING TECHNOLOGIES

ISSN 2454-9924 Volume: 1 Issue: 1(2015)

Here, we have identified two kinds of predictions:

1. ID-based prediction
2. Location-based prediction.

We say that a protocol for replica detection is ID-oblivious if the protocol does not provide any information on the ID of the sensors that will be the witnesses of the clone attack during the next protocol run. Similarly, a protocol is area-oblivious if probability does not depend on the geographical position of node in the network. Clearly, when a protocol is neither ID-oblivious nor area-oblivious, then a smart adversary can have good chances of succeeding, since it is able to use this information to subvert the nodes that, most probably, will be the witnesses.

3.3 Confirmation of Random Number

Random Key pre-distribution security scheme is implemented in the sensor network. That is, each node is assigned a number randomly with Time Stamp from Group Leader. Then the Group Leader will transmit Random Number (Encrypted with RSA algorithm) which was generated with respect to that Time Stamp to the Witness node. Witness node will now check the Random number which is generated with the User information. If both the data are matched then the Witness node will confirm that this node is Genuine.

3.4 **Verification of User information**

Each node is assigned an ID as individual once it is registered into the network and also an ID for the whole group (i.e.) Location ID is generated for each and every Location. That Node ID and Location ID are also appended with 1 (Encrypted with RSA algorithm). Then the Witness node will now check the node ID + Location ID which is generated with the User Information. If both the data are matched then the Witness node will confirm that this node with that Location is Genuine.

3.5 Replica Detection and Transfer

Only the Witness node confirms the Sender node, the data is send to the Destination, which is Genuine. If user specified information and the internal information are varied then the Witness node will identify that Cloning or some Mal

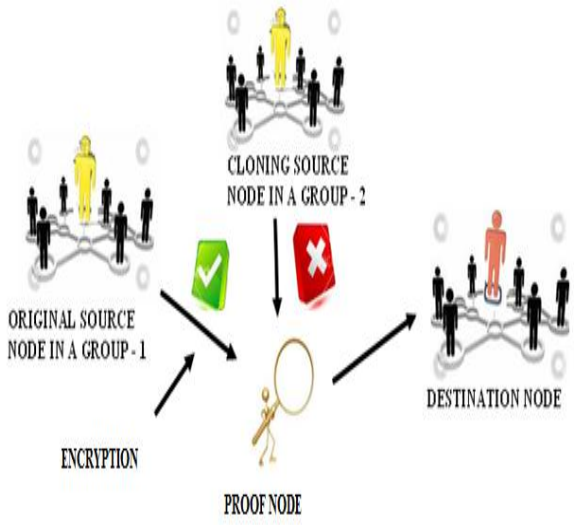
Copyright © 2015 IJARCSET. All rights reserved.

INTERNATIONAL JOURNAL OF ADVANCED RESEARCH IN COMPUTER SCIENCE AND ENGINEERING TECHNOLOGIES

ISSN 2454-9924 Volume: 1 Issue: 1(2015)

practice has occurred and the Packets are discarded by the witness node.

4 Architecture



From this architecture, it implemented with the following components, Original source node, cloning node, destination node, and the proof node. We provide a thorough empirical evaluation of effectiveness and efficiency of our proposed aggregation method. The results show that our method provides both higher accuracy and better collusion resistance than the existing methods.

5 Description of Algorithm

Input: a, b, c

Output: Estimation vector r

e→0, Q(0)→1;

Repeat

Calculate p(e+1)

Calculate f;

e→e+1;

Until estimation has processed

Here we assume that sensors are deployed in a hostile unattended environment. Consequently, some nodes can be physically compromised. We assume that when a sensor node is com- promised, all the information which is inside the node becomes accessible by the adversary. Thus, we cannot rely on cryptographic methods for preventing the attacks, since the adversary may extract cryptographic keys from the compromised nodes. We assume that through the compromised sensor nodes the adversary can send false data to the aggregator with a purpose of distorting the aggregate values. We also assume that all compromised nodes can be under control of

Copyright © 2015 IJARCSET. All rights reserved.

ISSN 2454-9924 Volume: 1 Issue: 1(2015)

a single adversary or a colluding group of adversaries, enabling them to launch a sophisticated attack. We also consider that the adversary has enough knowledge about the aggregation algorithm and its parameters. Finally, we assume that the base station and aggregator nodes cannot be compromised in this adversary model; there is an extensive literature proposing how to deal with the problem of compromised aggregators; in this paper we limit our attention to the lower layer problem of false data being sent to the aggregator by compromised individual sensor nodes, which has received much less attention in the existing literature.

6 Conclusion

From this Detection of Look Alike Detection of Clone Node and Collusion Attacks in WSN have been implemented, here we introduced a novel collusion attack scenario against a number of existing IF algorithms. Moreover, we proposed an improvement for the IF algorithms by providing an initial approximation of the trustworthiness of sensor nodes which makes the algorithms not only collusion robust, but also more accurate and faster converging. In future work, we will investigate whether our approach can protect against compromised aggregators. We also plan to implement our approach in a deployed sensor network.

7 References

[1] A. Jøsang and J. Golbeck, “Challenges for robust trust and reputation systems,” in Proc. 5th Int. Workshop Security Trust Manage., Saint Malo, France, 2009, pp. 253–262.

[2] B.-C. Chen, J. Guo, B. Tseng, and J. Yang, “User reputation in a comment rating environment,” in Proc. 17th ACM SIGKDD Int. Conf. Knowl. Discovery Data Mining, 211, pp. 159–167.

[3] C. de Kerchove and P. Van Dooren, “Iterative filtering in reputation systems,” SIAM J. Matrix Anal. Appl., vol. 31, no. 4, pp. 1812– 1834, Mar. 2010.

[4] C. T. Chou, A. Ignatovic, and W. Hu, “Efficient computation of robust average of compressive sensing data in wireless sensor networks in the presence of sensor faults,” IEEE Trans. Parallel Distrib. Syst., vol. 24, no. 8, pp. 1525–1534, Aug. 2013.

[5] D. Wagner, “Resilient aggregation in sensor networks,” in Proc. 2nd ACM

Copyright © 2015 IJARCSET. All rights reserved.

ISSN 2454-9924 Volume: 1 Issue: 1(2015)

Workshop Security Ad Hoc Sens. Netw., 2004, pp. 78–87.

[6] E. Ayday, H. Lee, and F. Fekri, "An iterative algorithm for trust and reputation management," Proc. IEEE Int. Conf. Symp. Inf. Theory, vol. 3, 2009, pp. 2051–2055.

[7] H. Liao, G. Cimini, and M. Medo, "Measuring quality, reputation and trust in online communities," in Proc. 20th Int. Conf. Found. Intell. Syst., Aug. 2012, pp. 405–414.

[8] H.-L. Shi, K. M. Hou, H. ying Zhou, and X. Liu, "Energy efficient
and fault tolerant multicore wireless sensor network: E MWSN," in Proc. 7th Int. Conf. Wireless Commun., Netw. Mobile Comput.,

[9] H.-S. Lim, G. Ghinita, E. Bertino, and M. Kantarcioglu, "A gametheoretic approach for high-assurance of data trustworthiness in sensor networks," in Proc. IEEE 28th Int. Conf. Data Eng., Apr. 2012, pp. 1192–1203.

[10] H.-S. Lim, Y.-S. Moon, and E. Bertino, "Provenance-based trustworthiness assessment in sensor networks," in Proc. 7th Int. Workshop Data Manage. Sensor Netw., 2010, pp. 2–7. 2011, pp. 1–4.

11] L. Wasserman, All of Statistics : A Concise Course in Statistical Inference. New York, NY, USA: Springer,.

[12] K. Hoffman, D. Zage, and C. Nita-Rotaru, "A survey of attack and defense techniques for reputation systems," ACM Comput. Surveys, vol. 42, no. 1, pp. 1:1–1:31, Dec. 2009.

[13] M. Rezvani, A. Ignjatovic, E. Bertino, and S. Jha, "Secure data aggregation technique for wireless sensor networks in the presence of collusion attacks," School Comput. Sci. and Eng., Univ. New South Wales, Kensington, NSW, Australia, Tech. Rep. UNSW-CSE-TR-201319, Jul. 2013.

[14] P. Laureti, L. Moret, Y.-C. Zhang, and Y.-K. Yu, "Information filtering via iterative refinement," Europhys. Lett., vol. 75, pp. 1006– 1012, Sep. 2006.

[15] R.-H. Li, J. X. Yu, X. Huang, and H. Cheng, "Robust reputation based ranking on bipartite rating networks," in Proc. SIAM Int. Conf. Data Mining, 2012, pp. 612–623.

Copyright © 2015 IJARCSET. All rights reserved.

ISSN 2454-9924 Volume: 1 Issue: 1(2015)

[16] R. Roman, C. Fernandez-Gago, J. Lopez, and H. H. Chen, "Trust and reputation systems for wireless sensor networks," in Security and Privacy in Mobile and Wireless Networking,S. Gritzalis, T. Karygiannis, and C. Skianis, eds.,Leicester, U.K.: Troubador Publishing Ltd, 2009 pp. 105–128,.

[17] S. Ozdemir and Y. Xiao, "Secure data aggregation in wireless sen- sor networks: A comprehensive overview," Comput. Netw., vol. 53, no. 12, pp. 2022–2037, Aug. 2009.

[18] Y.-K. Yu, Y.-C. Zhang, P. Laureti, and L. Moret, "Decoding information from noisy, redundant, and intentionally distorted sources," Physica A: Statist. Mech. Appl., vol. 371, pp. 732–744, Nov. 2006.

[19] Y. Yu, K. Li, W. Zhou, and P. Li, "Trust mechanisms in wireless sensor networks: Attack analysis and countermeasures," J. Netw. Comput. Appl., vol. 35, no. 3, pp. 867–880, 2012. 2

[20] Y. Zhou, T. Lei, and T. Zhou, "A robust ranking algorithm to spamming," Europhys. Lett., vol. 94, p. 48002, 2011.

Copyright © 2015 IJARCSET. All rights reserved.