IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 5, Issue 7, July 2016

Redundancy Management of Multipath Routing for Intrusion Tolerance in Hetrogeneous WSN

Manisha Dangi[1], Prof. R.K. Krishna[2]

Department of Computer Science &Engineering, RCERT, Chandrapur[1, 2]

Abstract: Wireless sensor networks (WSNs) are an important for monitoring distributed remote environments. As one of the key technologies involved in WSNs, nodes fault detection is indispensable in most WSN applications. It is well known that the distributed fault detection scheme checks out the failed nodes by exchanging data and mutually testing among neighbor nodes in this network., but the fault detection accuracy of a scheme would decrease rapidly when the number of neighbor nodes to be diagnosed is small and the node's failure ratio is high. an improved scheme is proposed by defining new detection criteria. Simulation results demonstrate that the improved scheme performs well in the above situation and can increase the fault detection accuracy greatly. wireless sensor-actor networks, sensors probe their surroundings and forward their data to actor nodes. Actors collaboratively respond to achieve predefined application mission. Since actors have to coordinate their operation, it is necessary to maintain a strongly connected network topology at all times. Moreover, the length of the inter-actor communication paths maybe constrained to meet latency requirement. Distributed Actor Recovery Algorithm (DARA) Most existing works mainly focus on the design of the trust models and how these models can be used to defend against certain insider attacks. However, these studies are empirical with the implicit assumption that the trust models are secure and reliable. In this paper, we discuss several security vulnerabilities that watchdog and trust mechanisms have, examine how inside attackers can exploit these security holes, and finally propose defending approaches that can mitigate the weaknesses of trust mechanism. We observe that many existing trust models adopting watchdog as their monitoring mechanism do not explicitly address these weaknesses. Our goal in this paper is to demonstrate how serious insider attacks can be in WSNs.

Keywords: Network security, virtual network system computing, intrusion detection, attack graph, zombie detection.

INTRODUCTION

An important security issue in wireless sensor network (WSN) because traditional security mechanisms, such as authentication and authorization, cannot catch inside attackers who are legal members of the network. Inside attackers can disrupt the network by dropping, modifying, or misrouting data packets. This is a serious threat for many applications such as military surveillance system that monitors the battlefield and other critical infrastructures.Trust mechanism with the notion of trust in human society has been developed to defend against insider attacks . Since WSNs consist of hundreds or thousands of tiny sensor nodes, the trust mechanism is often implemented as a distributed system where each sensor can evaluate, update, and store the trustworthiness of other nodes based on the trust model.

METHODOLOGY

To introduces significantly less messaging overhead to enable and during the recovery in comparison to the centralized version,. Actually, in the centralized version, each node must be aware of the complete network topology, which involves messages required for maintaining the network status, as pointed out earlier. Thus, the messaging overhead dramatically grows as the node count increases. On the other hand, requires maintaining one-hop neighbor information for performing the recovery. Thus, an extra N message overhead is considered for to exchange information initially at the network startup. Conversely, It averages the available route discovery process and does not impose prefigure messaging overhead. The only communication cost incurred during the recovery is when a node informs its children about its movement or broadcasts the successful relocation.

Nonetheless, as previously noted, the avoidance of explicit state update comes at the cost of increased travel overhead. It is important to note that for the results , no heartbeat messages are counted during the network operation for all approaches. In practice, heartbeat messages may or may not be explicitly transmitted. Typically, a node that stays quiet for a long time has to send a message to confirm its healthy status. Otherwise, messages that are part of the normal network operation, such as route update, data packet generation, inter-the coordination, etc., would suffice. We argue that the number of heartbeat messages would vary from node to node and over time. It is our view that they are not part of the recovery process in case a node failure is to be tolerated. Therefore, we did not fit in heartbeat messages in the results and the centralized approach. Path Length Validation Metrics:

It does not extend the shortest path between any pair of nodes. As expected, to achieves its design objective and does not extend any shortest path unlike shortest path and

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 5, Issue 7, July 2016

DARA. It engages all neighbors of the failed node and triggers subsequent cascaded relocation. This can be tolerated in sparse topologies. However, in highly connected networks, i.e., large N nodes are involved in the recovery process, as indicated by . As a result, the scope of node movement grows dramatically, and the number of extended paths increases, as On the other hand, DARA performs very close to highly connected topologies. In sparse networks, DARA does not do well with significant number of extended paths.

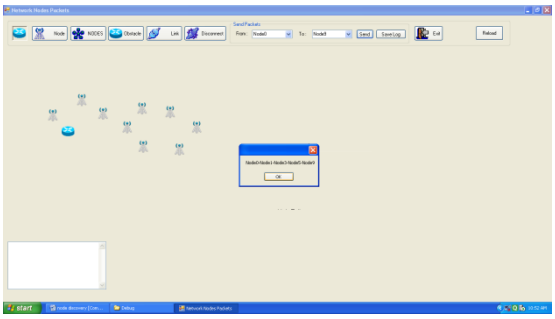

Fig1. Trust Path generation

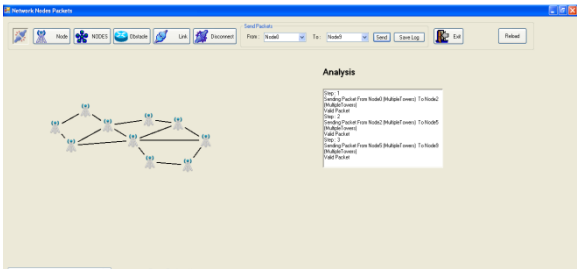

Fig 2. Path Regeneration

Research Methodology:
In general, trust mechanism works in the following stages.
1) Node behavior monitoring : Each sensor node monitors and records its neighbors' behaviors such as packet forwarding. This collected data will be used for trustworthiness evaluation in the next stage. Watchdog is a monitoring mechanism popularly used in this stage. The confidence of the trustworthiness evaluation depends on how much data a sensor collects and how reliable such data is.

2) Trust model defines how to measure the trustworthiness of a sensor node. introduced several representative approaches to build the trust model, which include Bayesian approach, Entropy approach, Game-theoretic approach, and Fuzzy approach. The trust value of a node may be different when we use different trust models. For example, when a node is observed to forward the packet stimes and drops the packet Insider trust Management Intelligent inside attacks against trust mechanism Vulnerabilities in the inside attacker detection stage Average End-to-End delay Packet Delivery Ratio Energy Consumption Multi-hop Chain Topology Inside attack detection : Based on the trust value, a sensor node determines whether its neighbor is trustworthy for collaboration (such as packet forwarding). If a neighbor's trust value is less than a certain threshold , it will be considered as an untrusted or malicious node. Depending on the WSN's trust mechanism, the detection of such insider attacker may or may not be broadcast to the rest of the nodes in the WSN. Moreover, we cannot keep aside the case of zero day attack where the vulnerability is discovered by the attacker but is not detected by vulnerability scanner. In such case, the alert being real will be regarded as false, given that there does not exist corresponding node in SAG. Thus, current research does not address how to reduce the false negative rate. It is important to note that vulnerability scanner should be able to detect most recent vulnerabilities and sync with the latest vulnerability database to reduce the chance of Zero-day attacks.

RESULTS AND DISCUSSION

The proposed algorithm has been carried out using the network simulator .net. To improved the version of recovery Scheme. Performances of the DARA, Shortest path are evaluated.

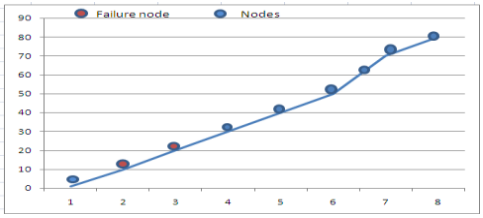

Fig: Multiple Nodes fail detection

The figure Multiple Node fail detection to detection of the failure nodes. The propose protocol detect the multiple failure nodes at a time. In routing path1 having8 nodes detects the 2 failure nodes, routing path2 having the15 nodes detects 3 failure nodes and routing path 3 having 25 nodes to detects 5 failure nodes. The propose protocol detects the more failure nodes very quickly. The propose protocol detection 80% failure node. The technique detect faster failure detects as compare to previous technique.

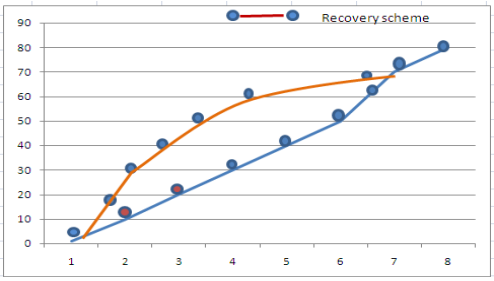

Fig: The recovery scheme

In routing path1 failure nodes are 2 apply the recovery scheme by 3 nodes. Routing path 2 detects 3 failure nodes apply the recovery scheme by nodes 5, so send the data from this 5 nodes. In routing path3 failure nodes are 5 so apply the recovery scheme by 7nodes. The propose

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 5, Issue 7, July 2016

protocol provide 90% faster recovery. To use of combinational methodology to provide faster recovery scheme. The delivery of the packet to the destination four times faster then the previous technique. To use the recovery scheme so that without dropping of message packet the data are deliver to the destination. To give the assurance of the data packet delivery. So that the life time of the network is maximize.

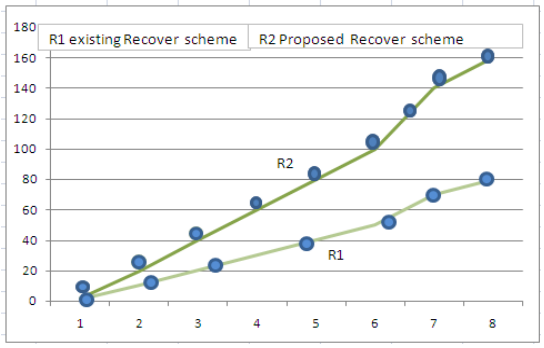

Fig: Comparing Recovery Scheme

The figure shows the comparing the recovery scheme of the existing system and the propose system. So the Combinational technique provides 8% more recovery from the existing system.

CONCULSION

A trust threshold can be designed in static manner or dynamic manner. Static trust threshold might be optimal only for limited cases that we consider in the simulation. As a result, it may not be good for unconsidered situations. Meanwhile, dynamic trust threshold that adaptively changes according to situations in our network may have reasonably good results, although it may not be optimal for all situations. However, since dynamic trust threshold will be frequently computed, it must be designed in an energy-efficient way. The implementation stage involves careful planning, investigation of the existing system and it's constraints on implementation, designing of methods to achieve changeover and evaluation of changeover methods.

REFERENCES

[1] Azahdeh Faridi et al, "Comprehensive Evaluation of the IEEE 802.15.4 MAC Layer Performance With Retransmissions," IEEE Transactions

[2] Tran Hoang Hai and Eui-Nam Huh, "Detecting Selective Forwarding Attacks in Wireless Sensor Networks Using Two-hops Neighbor nowledge," Seventh International Symposium on Network

[3] K. Hoffman, D. Zage, and C. Nita-Rotaru, "A survey of Attack and Defense Techniques for Reputation Systems," ACM Computing Surveys, Vol 41, Issue 4, 2009.

[4] H. Takabi, J.B. Joshi, and G. Ahn, "Security and PrivacyChallenges in Cloud Computing Environments," IEEE Security and Privacy, vol. 8, no. 6, pp. 24-31, Dec. 2010.

[5] "Open vSwitch Project," http://openvswitch.org, May 2012.

[6] Z. Duan, P. Chen, F. Sanchez, Y. Dong, M. Stephenson, and J.Barker, "Detecting Spam Zombies by Monitoring Outgoing Messages," IEEE Trans. Dependable and Secure Computing, vol. 9, no. 2, pp. 198-210, Apr. 2012.

[7] G. Gu, P. Porras, V. Yegneswaran, M. Fong, and W. Lee,"BotHunter: Detecting Malware Infection through IDS-driven Dialog Correlation," Proc. 16th USENIX Security Symp. (SS '07),

[8] G. Gu, J. Zhang, and W. Lee, "BotSniffer: Detecting Botnet Command and Control Channels in Network Traffic," Proc. 15th Ann. Network and Distributed Sytem Security Symp. (NDSS '08), Feb.2008.

[9] O. Sheyner, J. Haines, S. Jha, R. Lippmann, and J.M. Wing, "Automated Generation and Analysis of Attack Graphs," Proc. IEEE Symp. Security and Privacy, pp. 273-284, 2002,

[10] "NuSMV: A New Symbolic Model Checker," http://afrodite.itc.it:1024/nusmv. Aug. 2012.

[11] P. Ammann, D. Wijesekera, and S. Kaushik, "Scalable, graphbased network vulnerability analysis," Proc. 9th ACM Conf. Computer and Comm. Security (CCS '02), pp. 217-224, 2002.

[12] X. Ou, S. Govindavajhala, and A.W. Appel, "MulVAL: A Logic-Based Network Security Analyzer," Proc. 14th USENIX Security Symp., pp. 113-128, 2005.

[13] R. Sadoddin and A. Ghorbani, "Alert orrelation Survey: Framework and Techniques," Proc. ACM Int'l Conf. Privacy, Security and Trust: Bridge the Gap between PST Technologies and Business Services (PST '06),

[14] L. Wang, A. Liu, and S. Jajodia, "Using Attack Graphs for Correlating, Hypothesizing, and Predicting Intrusion Alerts," Computer Comm., vol. 29, no. 15, pp. 2917-2933, Sept. 2006.

[15] S. Roschke, F. Cheng, and C. Meinel, "A New Alert Correlation Algorithm Based on Attack Graph," Proc. Fourth Int'l Conf. Computational Intelligence in Security for Information Systems, pp. 58-67, 2011.

[16] A. Roy, D.S. Kim, and K. Trivedi, "Scalable Optimal Countermeasure Selection Using Implicit Enumeration on Attack Countermeasure Trees," Proc. IEEE Int'l Conf. Dependable Systems Networks (DSN '12), June 2012.