Accurate and lightweight intrusion detection system for identifying compromised nodes in WSN

Miss. Bhumanesh Fauzdar[1], Miss. Archana Singh[2]
[1]Apex Institute of Engineering and Tech.,Jaipur(Raj),
[2]Kautilya Institute of Engineering and Tech.,Jaipur(Raj)

Abstract

Wireless sensor networks (WSNs) are vulnerable to outer attack as they are deployed in open and unattended environments. Attacker can extract vital information, such as security keys, from compromised nodes and use them to launch insider attacks, so detecting when a node is compromised is important to securing WSNs. In this paper, we present , an accurate and lightweight intrusion detection system for identifying compromised nodes in wireless sensor networks. As we implement this system the benefits of this system is, it is not vulnerable to slander attacks, it has detection rates of 99% and false positive ratios of less than 2% in environments with loss rates of 30%, which is far more than existing systems, it has simple WSNs type features (sensor readings, receive power, send rate, and receive rate) and can adjust its detection behavior f the sensor application doesn't have periodic transmissions or lacks inter-node communication, and it has low memory, computation, and communication overheads that allows it to scale to networks of over thousands of nodes.

Keywords:wireless sensor network, ComSen: intrusion detection system.

I. Introduction

The sensor nodes are inexpensive and are autonomous in nature so use of wireless sensor network are expand to many of the areas like home automation, healthcare application, traffic control and many of the areas. Compared to traditional wired and wireless network the deployment is easy for sensor node. Also however, as WSNs expand to more security-critical applications like battle-field surveillance, securing them against adversaries becomes an important concern. Without security in hostile environments, it is impossible to trust the reports from WSNs.

The inexpensive and autonomous nature of sensor nodes, called motes very low cost low power computer and monitors the other nodes.

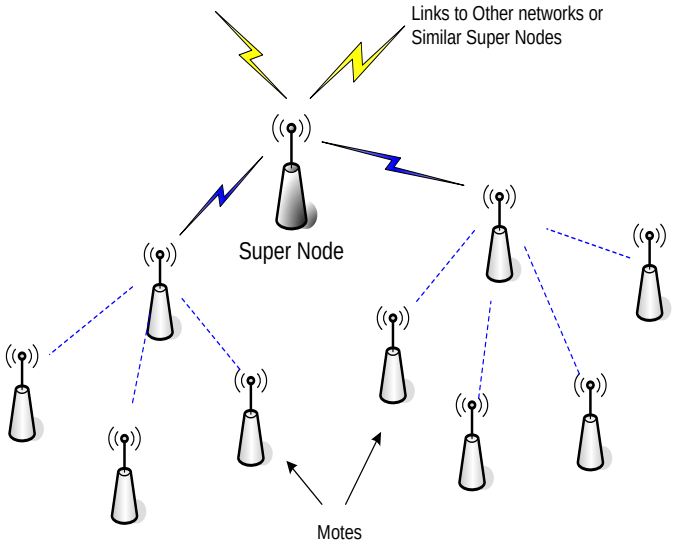


Fig1. WSN Structure

The inexpensive and autonomous nature of sensor nodes, called motes very low cost low power computer and monitors the other nodes. Wireless Sensor Network formed by many number of motes that communicate with each other and pass data along from one to another.

However, motes have limited resources, in terms of computational power, memory, and battery life, and are frequently deployed in open environments, so they are vulnerable to node compromise (where an adversary gains control of a node in the network). Without detection by the network, the compromised node is considered an authorized participant in the network and can launch insider attacks, which are attacks that leverage their higher access and authority.

There are following characteristic of Wireless Sensor Network:

Accuracy: Specifically, this requirement involves (1) a high detection rate, (2) a low false positive rate, and (3) a low detection time. A high detection rate means that most compromises are reported. Few false positives means that the majority of reported compromises are valid (i.e., they correspond to actual compromises) so actions against any reported compromised node can be taken with confidence. Lastly, a low detection time limits the malicious actions that can be performed by compromised nodes before they are detected.

Flexibility: We have assumptions about the underlying network as possible and can be used in the majority of deployments to detect compromises.

Robustness: Wireless Sensor network should be robust. Compromised nodes may attempt to undermine the detection system through malicious behavior, such as slander attacks, where they send false information that implicates legitimate nodes as compromised.

Scalability: Since motes have limited resources, applications with high overheads will interfere with other applications and decrease the lifespan of the mote. So it should be scalable. i.e life spam should be more.

II. Basic idea

Many issues in Wireless sensor Network have been studied by referring the papers which are mentioned below, in which some of the issues are packet droppers and modifiers, information capturing, and node compromise where where a sensor node can be completely captured and manipulated by the adversary.

In"**A Survey of Sensor Network Applications" [1]** by Ning Xu present a snapshot of the recent deployed sensor network applications and identify the research challenges associated with such applications.

In "**On the Difficulty of Software-Based Attestation of Embedded Devices**" by **Claudio Soriente** investigates the shortcomings of existing software-based attestation techniques. Author also present two generic attacks, one based on a return-oriented rootkit and the other on code compression. Software based attestation is a promising solution for verifying the trustworthiness of inexpensive, resource constrained sensors, because it does not require dedicated hardware, nor physical access to the device. In **"An RSSI-based Scheme for Sybil Attack Detection in Wireless Sensor Networks "[3]** author Murat Demirbas, Youngwhan Song present a robust and lightweight solution for Sybil attack problem based on received signal strength indicator (RSSI) readings of messages. In **"A Pairwise Key Pre-distribution Scheme for Wireless Sensor Networks"[4]** by Wenliang Du and Jing Deng proposed a new key pre-distribution scheme, which substantially improves the resilience of the network compared to the existing schemes. In **"Packet Leashes: A Defense against Wormhole Attacks in Wireless Networks"** [5]authors Yih-Chun Hu, Adrian Perrig and David B. Johnson explain about wormhole attack in wireless sensor network. In the wormhole attack, an attacker records packets (or bits) at one location in the network, tunnels them (possibly selectively) to another location, and retransmits them there into the network. The wormhole attack can form a serious threat in wireless networks, especially against many ad hoc network routing protocols and location-based wireless security systems. In "**The Sybil Attack in Sensor Networks: Analysis & Defenses"[6]** authors James Newsome, Elaine Shi, Dawn Song discuss about the Sybil attack in sensor network. In Sybil attack a node illegitimately claims multiple identities. In **"LITEWORP: A Lightweight Countermeasure for the Wormhole Attack in Multihop Wireless Networks"** authors Issa Khalil, Saurabh Bagchi, Ness B. Shroff discuss about wormhole attack where a malicious node records control and data traffic at one

location and tunnels it to a colluding node, which replays it locally.

III. Design phase:

Functional Requirements

Broadly, functional requirements define what a system is supposed to do whereas non-functional requirements define how a system is supposed to be. Functional requirements are usually in the form of "system shall do requirement", while non-functional requirements are "system shall be requirement".

1. Create sensor network with configurable number of nodes and the range of communication:In this part our main emphasis is to create a wireless sensor network of specified length with the specified number of nodes

2. Detect compromised nodes using Rule based detection:This is our main part. In this part we find the compromise node. For this we made binary tree. Also we will check the behavior of node. If past of node is not good it means behaviour of such node is suspicious and we have to careful for such node.

3. Rules can be configured based on sensor value, sending rate, receiving rate, send power.

After this we sent the data to the neighboring node. Also during this process sensor node need the power so power will also send. Some of the mark is also done on the packet.

4.When sensor sends data, the rules are matched and matching packets are dropped.

After getting the packet

5.Detect compromised nodes using Anomaly based detection.

6Measure the performance of Anomaly based detection by varying the sending rate and drawing the performance graph.

System Architecture

The Fig:2 describer the system architecture of the project, where modules implemented are Front End, Base Station, Detect compromised node, Rule Based Station, Anamaly Based Station.

We design the ComSen based on some of the following characteristic.

- **The network has densely deployed sensor nodes such that sensor nodes have overlapping sensing ranges and a given event is detected by multiple nodes. Since the ranges overlap, a sensor node can monitor the activities of its neighbors.**
- **Sensor nodes are motes with limited computation, communication, and energy resources.**

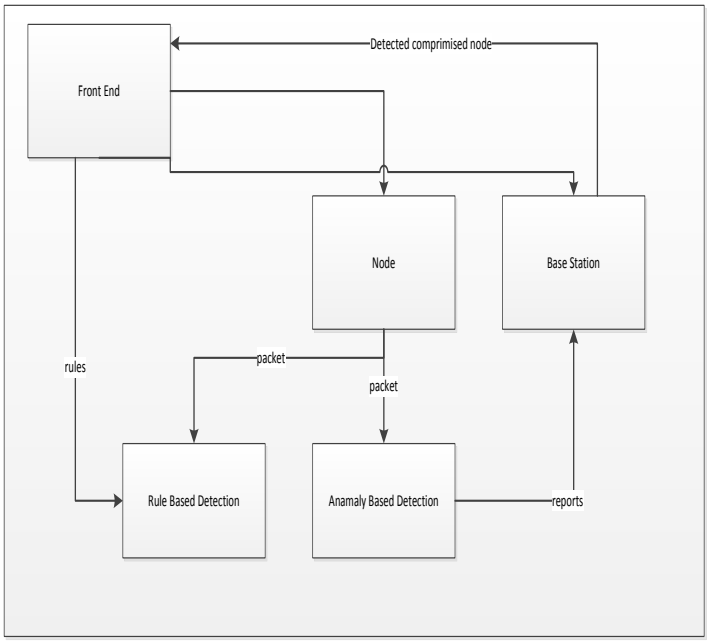


Fig 2. System Architecture

- There is a routing protocol used to forward messages between the base station and the nodes.
- Sensor nodes have unique identifiers so that the base station knows which reported compromise corresponds to which node.
- Compromised nodes can perform any number of attacks to degrade the network's security and performance, we focus on compromised nodes that perform malicious acts (i.e., launch insider attacks such as falsifying data).

The detection of misbehavior distributed component in ComSen is done by 5 algorithm which are:

1. Detection using sensor reading.
2. Detection using receive power.
3. Detection using send rate.
4. Detection using receive rate.
5. Detection using join messages.

IV. Rule Based technique

In the rule-based algorithm, if a node detects a new neighbor outside of the setup period, by hearing any messages from it. It will immediately consider the neighbor compromised.

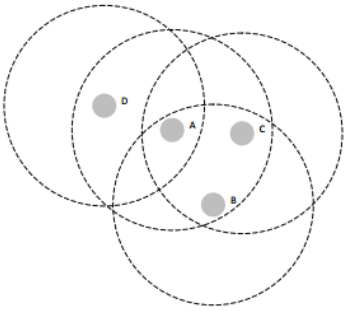


Fig 3.Rule Based Algorithm

These rules prevent compromised nodes, and even external attackers, from impersonating other nodes without being considered as new neighbors and reported. Figure 3 shows this property. Suppose node A was compromised and wants to impersonate another node. It cannot impersonate A or B without node D detecting a new neighbor. It cannot impersonate D without nodes B and C detecting a new neighbor. It cannot impersonate any other node except with B, C, and D detecting new neighbors. Thus, with enough neighbors monitoring each other, any attacks involving impersonation can be detected.

Working of Anomaly Based algorithm:

The four anomaly-based algorithms all follow a similar approach. Every node has two buffer for each monitored neighbor:

- Packet Buffer
- Misbehavior Buffer

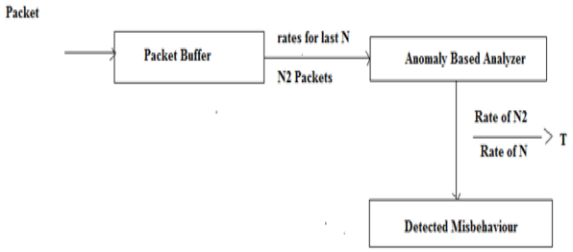


Fig 4. detection algorithms that use send receive rate

The algorithm that uses the sensor readings is almost identical to the one that uses the receive power. The only difference is that the difference between the node's and the neighbor's sensor readings is used instead of the receive power.

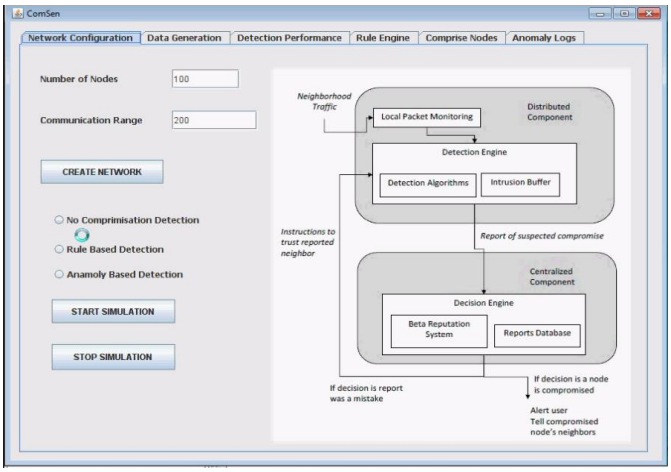
It calculates two rates: the rate at which the last N2 Packets are sent (including the last packet), rateN2 , and the rate at which the last N packets are sent, rate N where N > N2 . If the ratio of these two rates is above a threshold K the corresponding neighbor is considered to be compromised.

Rate of N2/Rate of N > K ……1

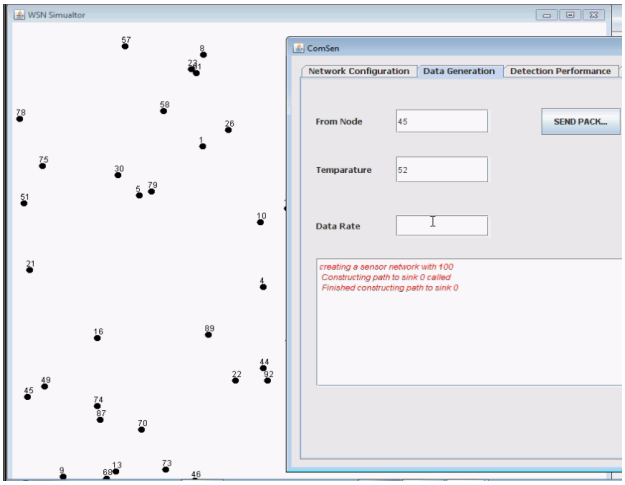
V. Implementation and Result:

Implementation is the stage of the project where the theoretical design is turned into a working system. At this stage the main workload and the major impact on the existing system shifts to the user department.

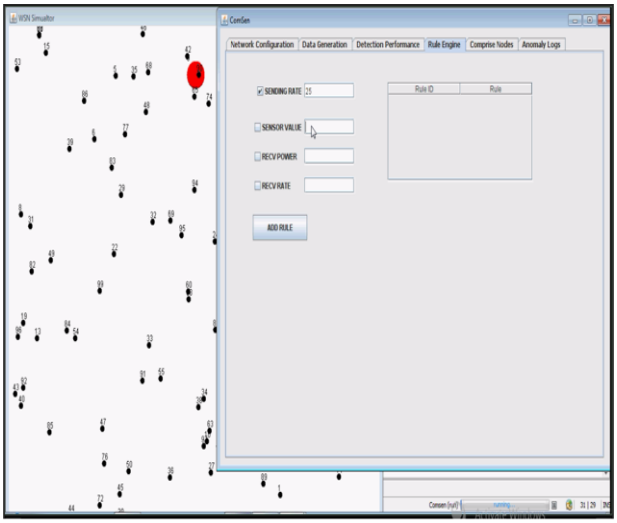
Step 1: Create network on number of nodes and communication range. Also we have options based on the Rule based detection and Anamoly Based detection.



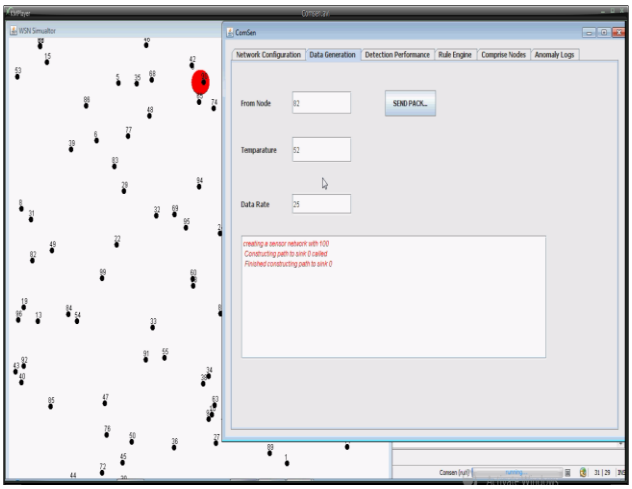
Step 2: In the following figure we set the different parameters like sink node number, originating node number, and set the data rate etc.



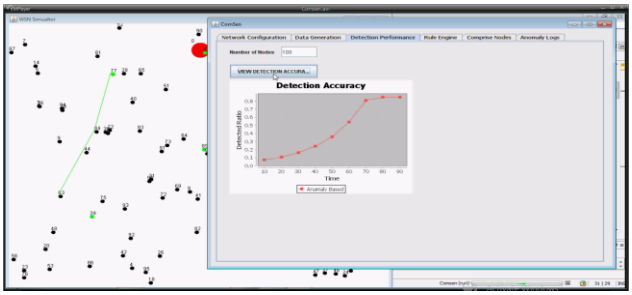
Step 3: In this step, based on user input node is generated. Also packet sending process is going on.



Step 5:After that at last we have created graph of detection accuracy.



Step 4: In this step rule engine is set. i.e Sending rate, sensor value, Recv power, receive rate etc are set.



VI. Conclusion:

In Wireless Sensor Network, compromised nodes can result in the the integrity of data by sending false data reports, injecting false data, and disrupting transmissions. So only cryptography are not sufficient to prevent these attacks, So we proposed ComSen, a system for detecting compromised nodes in WSNs Based on many of the parameters.

In this paper we have presented design and working of novel intrusion system ComSen which is not vulnerable to slander attack. In Slander attack malicious node use detection algorithm to launch different attacks. Also ComSen can run on different WSNs because it uses common application features (sensor readings, receive power, send rate, and receive rate) and can adjust its detection behavior if the sensor application doesn't have periodic transmissions or lacks inter-node communication. It has low memory, computation, and communication overhead.

.References:

[1] I. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci. A survey on sensor networks. Communications Magazine, IEEE, 40(8):102 – 114, Aug 2002.

[2] C. Castelluccia, A. Francillon, D. Perito, and C. Soriente. On the difficulty of software-based attestation of embedded devices. In CCS '09: Pro-ceedings of the 16th ACM conference on Computer and communications security, pages 400–409, New York, NY, USA, 2009. ACM.

[3] X. Chen, K. Makki, K. Yen, and N. Pissinou. Node compromise modeling and its applications in sensor networks. In Computers and Communications, 2007. ISCC 2007. 12th IEEE Symposium on, pages 575 –582, July 2007.

[4] B. E. Commerce, A. Jsang, and R. Ismail. The beta reputation system. In In Proceedings of the 15th Bled Electronic Commerce Conference, 2002.

[5] M. Conti, R. Di Pietro, L. V. Mancini, and A. Mei. A randomized, efficient, and distributed protocol for the detection of node replication attacks in wireless sensor networks. In Proceedings of the 8th ACM international symposium on Mobile ad hoc networking and computing, MobiHoc '07, pages 80–89, New York, NY, USA, 2007. ACM.

[6] M. Demirbas and Y. Song. An rssi-based scheme for sybil attack detection in wireless sensor networks. In Proceedings of the 2006 International Symposium on on World of Wireless, Mobile and Multimedia Networks, WOWMOM '06, pages 564–570, Washington, DC, USA, 2006. IEEEComputer Society.

[7] R. Di Pietro, L. V. Mancini, and A. Mei. Random key-assignment for secure wireless sensor networks. In Proceedings of the 1st ACM workshop on Security of ad hoc and sensor networks, SASN '03, pages 62–71, New York, NY, USA, 2003. ACM.

[8] D. Djenouri, L. Khelladi, and A. Badache. A survey of security issues in mobile ad hoc and sensor networks. Communications Surveys Tutorials, IEEE, 7(4):2 – 28, 2005.

[9] W. Du, J. Deng, Y. S. Han, P. K. Varshney, J. Katz, and A. Khalili. A pairwise key predistribution scheme for wireless sensor networks. ACM Trans. Inf. Syst. Secur., 8:228–258, May 2005.

[10] X. Du and H.-H. Chen. Security in wireless sensor networks. Wireless Communications, IEEE, 15(4):60 – 66, Aug 2008.

[11] S. Ganeriwal and M. B. Srivastava. Reputation-based framework for high integrity sensor networks. In In SASN 04: Proceedings of the 2nd ACM workshop on Security of ad hoc and sensor networks, pages 66–77. ACM Press, 2004.

[12] Y.-C. Hu, A. Perrig, and D. Johnson. Packet leashes: a defense against wormhole attacks in wireless networks. In INFOCOM 2003. Twenty-Second Annual Joint Conference of the IEEE Computer and Communica-tions. IEEE Societies, volume 3, pages 1976 – 1986 vol.3, Mar 2003.

[13] N. James, E. Shi, D. Song, and A. Perrig. The sybil attack in sensor networks: analysis & defenses. In Proceedings of the 3rd international symposium on Information processing in sensor networks, IPSN '04, pages 259–268, New York, NY, USA, 2004. ACM.

[14] I. Khalil, S. Bagchi, and N. B. Shroff. Liteworp: A lightweight countermeasure for the wormhole attack in multihop wireless networks. Dependable Systems and Networks, International Conference on, 0:612– 621, 2005.

[15] C. Krau, M. Schneider, and C. Eckert. On handling insider attacks in wireless sensor networks. Information Security Technical Report, 13(3):165 – 172, 2008.

[16] F. Li and J. Wu. Mobility reduces uncertainty in manets. In INFOCOM 2007. 26th IEEE International Conference on Computer Communications. IEEE, pages 1946 –1954, May 2007.

[17] Mica2. http://www.xbow.com/, June 2012.

[18] M. J. Miller and N. H. Vaidya. A mac protocol to reduce sensor network energy consumption using a wakeup radio. IEEE Transactions on Mobile Computing, 4:228–242, 2005.

[19] K. Okeya and T. Iwata. Side channel attacks on message authentication codes. In R. Molva, G. Tsudik, and D. Westhoff, editors, Security and Privacy in Ad-hoc and Sensor Networks, volume 3813 of Lecture Notes in Computer Science, pages 205–217. Springer Berlin / Heidelberg, 2005.

[20] I. Onat and A. Miri. An intrusion detection system for wireless sensor networks. In Wireless And Mobile Computing, Networking And Commu-nications, 2005. (WiMob'2005), volume 3, pages 253 – 259 Vol. 3, Aug 2005.

[21] B. Parno, A. Perrig, and V. Gligor. Distributed detection of node replication attacks in sensor networks. In Security and Privacy, 2005 IEEE Symposium on, pages 49 – 63, May 2005.

[22] A. Seshadri, M. Luk, and A. Perrig. Sake: Software attestation for key establishment in sensor networks. In DCOSS '08: Proceedings of the 4th IEEE international conference on Distributed Computing in Sensor Systems, pages 372–385, Berlin, Heidelberg, 2008. Springer-Verlag.
[23] A. Seshadri, M. Luk, A. Perrig, L. van Doorn, and P. Khosla. Scuba: Secure code update by attestation in sensor networks. In WiSe '06: Proceedings of the 5th ACM workshop on Wireless security, pages 85– 94, New York, NY, USA, 2006. ACM.
[24] A. Seshadri, A. Perrig, L. V. Doorn, and P. Khosla. Swatt: Software-based attestation for embedded devices. In In Proceedings of the IEEE
Symposium on Security and Privacy, 2004. [25] V. Shnayder, M. Hempstead, B.-r. Chen, G. W. Allen, and M. Welsh. Simulating the power consumption of large-scale sensor network applica-tions. In Proceedings of the 2nd international conference on Embedded networked sensor systems, SenSys '04, pages 188–200, New York, NY, USA, 2004. ACM.
[26] Y. L. Sun, Z. Han, W. Yu, and K. J. R. Liu. A trust evaluation framework in distributed networks: Vulnerability analysis and defense against attacks. In IEEE INFOCOM, pages 230–236, 2006.
[27] TinyOS. http://www.tinyos.net, June 2012.