International Journal of Modern Engineering Research (IJMER)
www.ijmer.com Vol.3, Issue.4, Jul - Aug. 2013 pp-1935-1938 ISSN: 2249-6645

Sender Authentication with Transmission Power Adjustment Method Using RSSI in Wireless Sensor Network

Archana Arudkar[1], Prof. Vimla Jethani[2]
*(Computer Department, RAIT / Mumbai University, India)
** (Computer Department, RAIT / Mumbai University, India)

Abstract: *With the advent of powerful and efficient wireless sensor nodes, the usage of wireless sensor networks (WSN) has been increased greatly. Sensor networks consist of a network of autonomous sensors that can reconfigure themselves so as to sense the environment in the most efficient manner. These nodes are having low power and limited range. Low power implies limited battery life. In WSN, to perform the task successfully low energy consumption is the major concern. Wide use of WSN in practical application makes it necessary to maintain the network security.IP or MAC addresses are used for sender authentication which can be spoofed easily. This makes these types of networks vulnerable to many identity-based attacks. To protect wireless network from such type of attacks, Received Signal Strength Indicator (RSSI) value called 'Signalprint' can be used for sender authentication, which is harder to spoof. However in WSN battery discharge causes received signal characteristics to vary. This may give false alarm in sender authentication. Low energy consumption is one way to mitigate this problem.*

Keyword: *Received Signal Strength Indicator, Signalprint, Sender Authentication, Transmission Power, Wireless Sensor Network.*

I. INTRODUCTION

A wireless sensor network consists of spatially distributed autonomous sensors to cooperatively monitor physical or environmental conditions, such as temperature, sound, vibration, pressure, motion. The development of wireless sensor networks (WSN) was motivated by military applications such as battlefield surveillance. It is now used in many industrial and civilian application areas, including industrial process monitoring and control, machine health monitoring, environment and habitat monitoring, healthcare applications, home automation and traffic control.

A sensor node, also known as a mote is a node in a WSN that is capable of performing some processing, gathering sensory information and communicating with other connected nodes in the network. Therefore the success of WSN depends on the ability of the member nodes of the network to co-operate among them. Due to this high level of co-operation required, WSNs are susceptible to many security attacks from intruders. In the absence of security mechanism, attackers are getting success to degrade the performance of the network and even bring down the network. To provide the security to WSN needs to separate the nodes of the intruders from the member nodes. To separate the intruder's node from legal member nodes needs to identify the member nodes in the network. Presently IP or MAC addresses are used to identify the node, which is vulnerable to spoofing. [1] proposes a method that uses the sent data characteristics called Received Signal Strength Indicator (RSSI) to identify the sender. The characteristic of the signal at the receiver depends on factors such as attenuation, atmospheric conditions and intervening obstacles. This makes it hard for the receiver to alter the transmitted signal characteristics so as to masquerade as another node. RSSI value captured at several different nodes is aggregated and a signalprint is generated for the sender. This provides security from the identity based attacks like Masquerading and Resource Depletion attacks. RSSI value proves very good identifying characteristics for a node in WSN, where little or no mobility of the node occurs. A node in a WSN has limited battery life. As the battery discharges the intensity of the transmitted signal also reduces. The transmission power of the sensor node reduces with the supply voltage of the battery [4].This affects the RSSI values which may raise a false alarm. To overcome from this problem, in WSNs, transmission power adjustment using RSSI is one way to minimize energy consumption and prolong the battery life and thus the network lifetime.

II. ATTACKS ON WSN

2.1Resource Depletion Attacks

This is essentially a Daniel of Service (DoS) attack. The attacker floods the network with unnecessary requests, thereby consuming large amount of network bandwidth, computational power and memory. The attacker goes one step ahead and attempts to mask its identity by spoofing its IP or MAC address. So it is difficult to detect. However, as signalprints are hard to spoof, a mechanism based on signalprints can detect such an attack.

2.2Masquerade Attacks

In a masquerade attack, the attacker poses as a valid member node. Most techniques involve spoofing IP or MAC address, so as to acquire the privileges of another valid member node. This allows the attacker to enter and access a network to which he is not authorized. Identity-based security mechanisms that use IP or MAC address – or any information that the sender sends as a part of data – cannot detect such security violations. The properties of signalprint makes it possible to detect this attack[1].

III. SIGNALPRINT

RSSI value is used to identify the sender. But the single value of RSSI is not sufficient to identify a sender. Multiple RSSI values are used for the sender's identity.

3.1 Received Signal Strength Indicator (RSSI)

RSSI is an indication of the power level being received by the antenna. Generally, the higher the RSSI level, the stronger is the signal. We can say that RSSI is used to indicate strength of the incoming signal in a receiver. (The signal strength indicator on a cell phone display is a common example.).RSSI is defined as ten times the logarithm of the ratio of power of the received signal and a reference power (e.g. 1mW) i.e., RSSI α 10 log P/Pref.This means RSSI α log P [5].It is a known fact that power dissipates from a point as it moves further out. So the relationship between power and distance is that power is inversely proportional to the square of the distance travelled. In other words:

$$RSSI \alpha \log (1/distance^2) \quad \ldots\ldots\ldots\ldots\ldots(1)$$

The RSSI values are highly dependent on environment phenomena. This dependence of RSSI values on the environmental phenomena makes it extremely difficult for the intruder to spoof RSSI values.

3.2 Signalprint Properties

Following are the properties of signalprint

- Signalprints are hard to spoof- The transmitted signal attenuation depends on the distance ,environmental factors and obstacles such as walls,furnitures.As the transmitter has no control on the environmental factor and thus unable to change the produced signalprint.
- Signalprint are strongly correlated with the physical location of the client.
- RSSI value from particular sender will not show a large difference from the initial RSSI value received [2].

3.3 Signal print Representation

-50	**-78**	**-36**	**-65**	**-46**

Fig1. Signal print Representation

Figure 1 shows the typical signalprint representation. A signal print is a vector of RSSI values received at different nodes for the same message transmitted for the same sender. The vector contains one entry for each receiver.

3.4 Signalprint Generation

The RSSI measured at a single receiver is not enough to uniquely identify the sender. However, a set of RSSI values taken at multiple receivers can uniquely and accurately identify the sender. Therefore, it is required to aggregate the individual RSSI values from multiple locations into a single signalprint vector. In [2], RSSI values measured at multiple 802.11 access points were sent to a central wireless appliance. The wireless appliance then acted as a central authority to generate and compare the signalprints. In a WSN, however, there is no natural centralized node. Therefore, a distributed approach is used. Each node in the network can obtain the RSSI values measured at the other nodes and generate the complete signalprint from these. When a signalprint generation is requested, all the nodes in the range of the sender measure the RSSI value corresponding to a transmission by the sender. These RSSI values are then passed on to all the neighbours along with a signature of the received message, so as to match the RSSI values with the received message. When a node receives the RSSI values from the other nodes, it places each RSSI value in its corresponding location in the signalprint vector .The greater the number of receivers collaborating to generate the signalprints, the greater is the number of RSSI values captured and, hence, the greater is the accuracy of the signalprint in identifying the receiver. Therefore, it is important to have as many receivers as possible. It is also observed that as the distance between the transmitter and the receiver increases, the sensitivity of the RSSI to changes in distance reduces. Hence, we would like the receiver to be close to the sender.

3.5 Differential Values

In order to identify the sender, we need to compare the generated signalprint with the previously stored signalprint for the vector. However, before comparing the signalprints ,convert each signalprint into differential values.Signalprints are either written with absolute or differential values: for example, a signalprint S1: (-50,-62,-76) written using differrential signal strength becomes S1: (0,-12,-26).The use of differential values increase the robustness of signalprint operations against devices that vary their transmission power levels between frames. With absolute values, changes in transmission power create similar changes in the detected RSSI, which could cause the system to attribute multiple packets sent by single client to multiple devices. Using differential values, transmissions performed by a stationary transmitter generate similar signalprints, increasing chances of attack detection [1].

IV. TRANSMISSION POWER ADJUSTMENT METHOD

To avoid identity based attacks on WSN [1] suggest the signalprint method using RSSI for sender authentication which is hard to spoof. There is a variation in RSSI value because of environmental condition, obstacles found in propagation, transmission power used and the discharge of battery. This work considers the battery drainage problem. The

variation in RSSI value occurs because of low battery power, gives false alarm in sender authentication. So this work compares the signalprint method for sender authentication with and without Transmission Power Adjustment which reduces false alarm by low energy consumption and hence better sender authentication.
In WSN, due to power limitations, transmission power adjustment using RSSI is way to minimize energy consumption and extend the battery life of sensor nodes. To minimize the power consumption, a node of should transmit each packet with the minimum power required for successful transmission.

All nodes are not pre-configured. Therefore, self-configuration is useful and practical way to gain useful information such as neighbour nodes. When a node is power on, its neighbour table is empty. So each node must send a wireless query to detect its neighbouring node so that it can communicate with it directly. This is called Neighbour Discovery process. To discovery of a neighbouring node, instead of sending many messages send only one message with maximum transmission power. Run this neighbor discovery process periodically to note down the updated RSSI value. To dynamically adjust the transmission power such that it will reduce the energy consumption without packet loss.
The minimum transmission power for sending a message from node x to node y is calculated using RSSI is:

We know that,

$$\text{RSSI (dBm)} = A - n \log d \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots.. (2)$$

Where A – transmission power
n – Propagation constant
d – Distance between sender and receiver node

If $P(x)$ – transmission power of x
$P_{max}(x)$ - maximum transmission power of node x
$P_{min}(x, y)$ - minimum transmission power required for node x to communicate with node y.

Put $A = P_{max}(x)$ in (2)

Therefore,

$$RSSI_{max}(x, y) = P_{max}(x) - 10n\log d \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots (3)$$

Put A = Pmin(x,y) for minimum transmission power

$$RSSI_{min}(x, y) = P_{min}(x, y) - 10n\log d \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots.. (4)$$

(5) is calculated by performing (4)-(3)

$$Pmin(x, y) = RSSI_{max}(x, y) - RSSI_{min}(x, y) + P_{max}(x) \ldots\ldots\ldots. (5)$$

Here values of $RSSI_{min}(x, y)$ and $P_{max}(x)$ obtained from device datasheet for CC2431 their values are -92dBm and 0 respectively.
To find the value of $RSSI_{max}(x, y)$, x sends a message using node's maximum transmission power to y and y will send back the message of $RSSI_{max}(x, y)$ value.
The variation in RSSI value is calculated as $RSSI_{delta}$ and included in (6) for error adjustment.

$RSSI_{delta}$ is calculated by using the difference between the maximum, Max ($RSSI_{max}(x,y)$) and minimum, Min($RSSI_{min}(x,y)$)

$$RSSI_{delta} = Max\,(RSSI_{max}(x, y)) - Min\,(RSSI_{min}(x, y)) \ldots\ldots\ldots\ldots\ldots\ldots... (6)$$

Therefore,

$$P_{min}(x, y) = RSSI_{max}(x, y) - RSSI_{min}(x, y) + P_{max}(x) + RSSI_{delta} \ldots\ldots\ldots.(7)$$

Suppose sender node is x and receiver node is y.Sender x broadcast a hello packet with maximum transmission power to receiver node y.Then receiver y replies a unicast message with $RSSI_{max}$ (x,y) to x. After that, x adds y and $RSSI_{max}$ (x, y) in its neighbour table. This process will be repeated periodically for updating $RSSI_{max}$ value during packet transmission. As mentioned in (7), minimum transmission power for sending messages from x to y is computed and adjusted to the closest transmission power level which is greater than or equal to the computed one.
By using the above transmission power, it was found that

- Packet loss rate of sending with power adjustment does not to be significantly different from sending with maximum power.
- Energy consumption for sending packet is reduced around 50% for all distances [6].

V. CONCLUSION

Signalprint using RSSI technique for sender authentication helps to detect Identity based attacks. As RSSI is hard to spoof and strongly associated with the location of the node, it is good option for sender authentication where less or no mobility occurs.

In WSN energy consumption is the major concern. More the energy consumption less is the battery life and hence the network life .Low battery power affects the RSSI value which may give false alarm. Transmission power adjustment is one method to improve the result. It is a known fact that most of the energy is consumed during neighbour discovery process.

Neighbour discovery is very important in wireless sensor networks. Many processes, such as topology-control, medium access control, and routing, rely on the information provided by the ND process. The RSSI value is one of the useful information for transmission power adjustment. This testbed uses RSSI value to estimate minimum transmission power for sending each packet to a neighbour node. Since reducing transmission power may raise the unsuccessful sending and receiving messages, dynamic adjustments of output power control is done by periodically sending a hello message to the neighbour and then receiving the current feedback RSSI value from that neighbour. Comparing to transmission with the maximum power, the testbed results show that the energy consumption in transmission process is significantly decreased, while the packet loss rate is not significantly different.

References

[1] Sudip Misra,Ashim Ghosh,A.P.Sagar P.,Mohammad S.Obaidat**,** Detection of Identity-Based Attacks in Wireless Sensor Networks Using Signalprints**,***2010 IEEE/ACM International Conference on Green Computing and Communication & 2010 IEEE/ACM International Conference on Cyber, Physical and Social Computing.*

[2] D.B. Faria and D.R. Cheriton,Detecting Identity Based Attacks In Wireless Networks using Signalprint**,** *Proceedings of the 5th ACM workshop on wireless security, Los Angeles, California, Sept 29, 2006.*

[3] K.Srinivasan and P. Levis, RSSI Is Under Appreciated**,** *in Proceedings of the 3th ACM workshop on Embedded Networked Sensors, May 2006.*

[4] S.Hussain and M.S. Rahman, Using Received Signal Strength Indicator to Detect Node Replacement and Replication Attacks in Wireless Sensor Networks, *in SPIE Proceedings on Data Mining, Intrusion Detection, Information Assurance and Data Networks.*

[5] Ambili Thottam Parameswaran,Mohammad I.Husain,Shambhu Upadhyaya, Is RSSI a Reliable Parameter in Sensor Localization Algorithms-An Experimental Study**,** *in field failure data analysis workshop, Niagara Falls,USA, September 2009*

[6] Wilawan Rukpakavong,Iain Phillips,Lin Guan, Neighbour Discovery for Transmit Power Adjustment in IEEE 802.15.4 using RSSI, New Technologies, Mobility and Security(NTMS),2011 4th IFIP International Conference on Feb-2011.