ISSN:2348-2079

Volume-6 Issue-2

International Journal of Intellectual Advancements and Research in Engineering Computations

Scale-Free Wireless Sensor Networks for Robustness Strategy

[1]Mr. S.Jagadeesan, M.Sc., MCA, ME, Assistant Professor,
[2]Ms. N. Johncy, Final MCA,
Department of MCA, Nandha Engineering College (Autonomous), Erode 52.
E-Mail ID: jagadeesan12398@gmail.com, johncynagaraj@gmail.com

***Abstract*-It is improving the robustness of the network topologies for WSNs. Itisdefine the terms of target selection for attacks, there are two types of attack: random and malicious. In random attacks, the attacker randomly chooses nodes in the network topology as the targets, whereas in malicious attacks, the attacker chooses the nodes with high node degrees as the targets. It is known that some types of network topologies are resistant to random attacks and some are resistant to malicious attacks. To use spatial information, a physical property associated with each node, hard to falsify, and not reliant on cryptography, as the basis for 1) detecting attacks; 2) determining the number of attackers when multiple adversaries masquerading as the same node identity; and 3) localizing multiple adversaries. It is proposed to use the spatial correlation of received signal strength (RSS) inherited from wireless nodes to detect the attacks.**

***Index Terms*—Signal strength, attacks, sensor networks, interval, scenario.**

I. INTRODUCTION

Sensor networks are deployed to sense, monitor, and report events of interest in a wide range of applications including, but are not limited to, military, health care, and animal tracking. In many applications, such monitoring networks consist of energy constrained nodes that are expected to operate over an extended period of time, making energy efficient monitoring an important feature for unattended networks. In such scenarios, nodes are designed to transmit information only when a relevant event is detected (i.e., event-triggered transmission).

The first step toward achieving source anonymity for sensor networks in the presence of global adversaries is to refrain from event-triggered transmissions. To do that, nodes are required to transmit fake messages even if there is no detection of events of interest. When a real event occurs, its report can be embedded within the transmissions of fake messages. Thus, given an individual transmission, an observer cannot determine whether it is fake or real with a probability significantly higher than 1/2, assuming messages are encrypted.

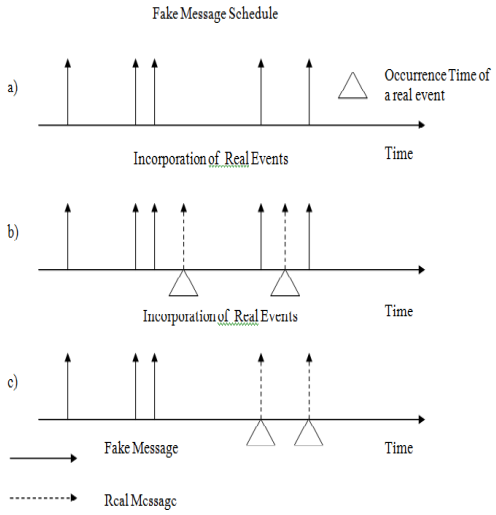

Fig 1.1 Message schedule Diagram

Different approaches for embedding the report of real events within a series of fake transmissions; (a) shows the prespecified distribution of fake transmissions, (b) illustrates how real events are transmitted as soon as they are detected, (c) illustrates how nodes report real events instead of the next scheduled fake message.

II. RELATED WORKS

In this paper[1], the authors Basel Alomair, Andrew Clark, Jorge Cuellary, and RadhaPoovendran were stated that the Preserving source location privacy is becoming one of the most interesting problems in wireless sensor networks. In a variety of real life applications, such as the deployment of sensor nodes in battlefields, the locations of events monitored by the network are required to remain anonymous. Given the knowledge of the network topology, however, an adversary can expose the locations of such events by determining the individual nodes reporting them

In this paper [3], the authors Basel Alomair, Andrew Clark, Jorge Cueller, and RadhaPoovendran were stated that investigate the security of anonymous wireless sensor networks. To lay down the foundations of a formal framework, they proposed a new model for analyzing and evaluating anonymity in sensor networks. The novelty of the proposed model is twofold: first, it introduces the notion of "interval indistinguishability" that is stronger than existing notions; second, it provides a quantitative measure to evaluate anonymity in sensor networks.

In this paper [9], the authors Adrian Perrig, Robert Szewczyk, j.d.Tygar, Victor Wen and David e. culler were stated that wireless sensor networks will be widely deployed in the near future. While much research has focused on making these networks feasible and useful, security has received little attention. They present a suite of security protocols optimized for sensor networks: SPINS.

SPINS has two secure building blocks: SNEP and TESLA. SNEP includes: data confidentiality, two-party data authentication, and evidence of data freshness. TESLA provides authenticated broadcast for severely resource-constrained environments. To implemented the above protocols, and show that they are practical even on minimal hardware: the performance of the protocol suite easily matches the data rate of the network. Additionally, it demonstrated that the suite can be used for building higher level protocols.

In this paper[4], the authors Deukjo Hong1, Jaechul Sung2, Seokhie Hong1, Jongin Lim1, Sangjin Lee1, Bon-Seok Koo1, Changhoon Lee1, Donghoon Chang1, Jesang Lee1, Kitae Jeong1, Hyun Kim4, Jongsung Kim1, and Seongtaek Chee were stated that the proposed a new block cipher HIGHT with 64-bit block length and 128-bit key length. It provides low-resource hard-ware implementation, which is proper to ubiquitous computing device such as a sensor in USN or a RFID tag. HIGHT does not only consist of simple operations to be ultra-light but also has enough security as a good encryption algorithm.

In this paper[10], the authors were stated that With the establishment of the AES the need for new block ciphers has been greatly diminished ; for almost all block cipher applications the AES is an excellent and preferred choice. However, despite recent implementation advances, the AES is not suitable for extremely constrained environments such as RFID tags and sensor networks. In this paper they describe an ultra- lightweight block cipher, present. Both security and hardware efficiency have been equally import ant during the design of the cipher and at 1570 GE, the hardware requirements for present are competitive with today's leading compact stream ciphers.

In this paper[10], the authors Min Shao, Yi Yang, Sencun Zhu, Guohong Cao were stated that the For sensor networks deployed to monitor and report real events, event source anonymity is an attractive and critical security property, which unfortunately is also very difficult and expensive to achieve. This is not only because adversaries may attack against sensor source privacy through traffic analysis, but also because sensor networks are very limited in resources. As such, a practical tradeoff between security and performance is desirable.

In this paper[8], the authors CelalOztur k, Yanyong Zhang, Wade Trappe were stated that the As sensor-driven applications become increasingly integrated into lives, issues related to sensor privacy will become increasingly important. Although many privacy-related issues can be addressed by security mechanisms, one sensor net-work privacy issue that cannot be adequately addressed by network security is confidentiality of the source sensor's location.

In this paper, to focus on protecting the source's location by introducing suitable modifications to sensor routing protocols to make it difficult for an adversary to backtrack to the origin of the sensor communication. In particular, focus on the class of flooding protocols. While developing and evaluating the privacy-aware routing protocols, to jointly consider issues of location-privacy as well as the amount of energy consumed by the sensor network.

In the paper[10], the authors Y. Ouyang, Z. Le, G. Chen, J. Ford, F. Makedon, and U. Lowell were stated that the Sensor networks are used in a variety of application areas for diverse problems from habitat monitoring to military tracking. Whenever they are used to monitor sensitive objects, the privacy of monitored objects' locations becomes an important concern. When a sensor reports a monitored object by sending a series of messages through the sensor network, the route these messages take in theory creates a trail leading back to their source.

III.SYSTEM METHODOLOGY

A. INTERVAL INDISTINGUISHABILITY

Statistical anonymity in sensor networks is modeled by the adversary's ability to distinguish between real and fake transmissions by means of statistical analysis. That is, given a series of transmissions of a certain node, the adversary must be unable to distinguish, with significant confidence, which transmission carries real information and which transmission is fake, regardless of the number of transmissions the adversary may observe.

Consider now an adversary observing a sensor network over multiple time intervals. Assume that, during a given time interval, the adversary is able to notice a change in the statistical behavior of transmission times of a certain node in the network. This distinguishable change in the transmission behavior of the node can be indicative of the existence of real activities detected and reported by that node during that interval, even if t he adversary was unable to distinguish between individual transmissions.

Definition 1 (Interval indistinguishability): Let IF denotes a time interval without any real event transmission (called the "fake interval" for the rest of the paper), and IR denotes a time interval with real event transmissions (called the "real interval" for the rest of the paper). The two time intervals are said to be statistically indistinguishable if the distributions of inter transmission times during these two intervals cannot be distinguished with significant confidence.

B. INTERVAL VERSUS EVENT INDISTINGUISHABILITY

However, in the m ore general scenario, in which intervals contain more than a single transmission, interval indistinguishability, implies indistinguishability of individual transmissions. To see this, assume a system satisfying interval indistinguishability but does not satisfy individual event indistinguishability. Since real and fake transmissions are distinguishable, given a fake interval and a real interval, the real interval can be identified as the one with the real transmission; a contradiction to the hypothesis that the system satisfies interval indistinguishability. That is, if intervals are in distinguishable, then individual events within them must also be indistinguishable.

In binary hypothesis testing, given two hypothesis, H0 and H1, and a data sample that belongs to one of the two hypotheses (e.g., a bit transmitted through a noisy communication channel), the goal is to decide to which hypothesis the data sample belongs. In the statistical strong anonymity problem under interval inistinguishability, given an interval of inter-transmission times, the goal is to decide whether the interval is fake or real (i.e., consists of fake transmissions only or contains real transmissions).

Given Definition 1 of interval indistinguishability, consider the following game between a challenger, C (the system designer), and a statistical adversary, A

Game 1: (Anonymity game).

- C chooses two intervals IR and IF, in which IR is a real interval and IF is a fake one.
- C draws a **bit** b $\in$ {0, 1} uniformly at random and sets IR ¼Ib and IF ¼Ib, where b denotes the binary complement of b.
- C gives I_b and I_{b^-} to A.
- A makes any statistical test of her choice on I_b and I_{b^-} and outputs a bit b'.
- If b'= b, A wins the game.

Game 1 can be viewed as a standard binary hypothesis testing problem. That is, given two hypotheses (a real interval and a fake interval) and an observed data (an interval of inter-transmission times of a sensor node), the goal of the adversary is to determine to which hypothesis the observed data belong (i.e, whether the observed interval contains real event transmissions).

C. STATISTICAL GOODNESS OF FIT TESTS AND THE SSA PROBLEM

1. SSA Solutions Based on Statistical Goodness of Fit Tests

The statistical goodness of fit of an observed data describes how well the data fits a given statistical model. Measures of goodness of fit typically summarize the discrepancy between observed values and the values expected under the statistical model in question. Such measures can be used, for example, to test for normality of residuals, to test whether two samples are drawn from identical distributions, or to test whether outcome frequencies follow a specified distribution**.**

2. Statistical Goodness of Fit under Interval Indistinguishability

In this section, they are analyzing for statistical goodness of fit-based solutions under the proposed model of interval indistinguishability. As before, let Xi be the random variable representing the time between the i^{th} and the $(i + 1)^{st}$ transmissions and let the desired mean of these random variables be μ; i.e., IE [Xi] = μ, for all i (since the Xi's are iid). We now examine two intervals, a fake interval and a real one.

3. Fake Interval (I_F)

Recall that, in the absence o f real events, nodes are programmed to transmit iid fake messages according to a pre-specified probability distribution.

That is, the (Xi S) in fake intervals are iid random variables with mean μ. Therefore, during any fake interval, I_F, for any $X_{i-1,}$ Xi $\in I_F$, one gets by the fact that Xi_{-1} andXi are independent by definition and that IE [Xj] =μ, for all j's.

$$IE [Xi \mid X_{i-1}<\mu] =\mu,$$

4. Real Interval (I_R)

By definition, real intervals will have both fake and real transmissions. Let E_i be the random variable representing the type of the event reported in the i^{th} transmission, i.e., fake or real. Then, E_i can take the values R and F, where R denotes a real event and F denotes a fake one. Since, in the most general scenario, the distribution of inter arrival times of real events can be time variant and unknown beforehand, we will assume that E_i can take the values R and F with arbitrary probabilities**.**

Recall that the time between the transmission of a real event and its preceding fake one is usually shorter than the mean,μ, by design (to reduce delay). Recall further that the time between the transmission of a real event and its successive one is usually longer than μ by design (to adjust the ensemble mean). That is, during any real interval, I_R, for any $X_{i-1,}$ Xi $\in I_{R,}$ one gets

$$IE [Xi \mid X_{i-1}<\mu, E_i= R] >\mu \text{ and } IE [Xi \mid X_{i-1}<\mu, E_i= F] = \mu$$

An inter-transmission time can be either shorter or longer than μ. For the rest of the paper, we call an inter-transmission time that is shorter than μ "short inter-transmission time" and an inter-transmission time that is longer than μ "long inter-transmission time."

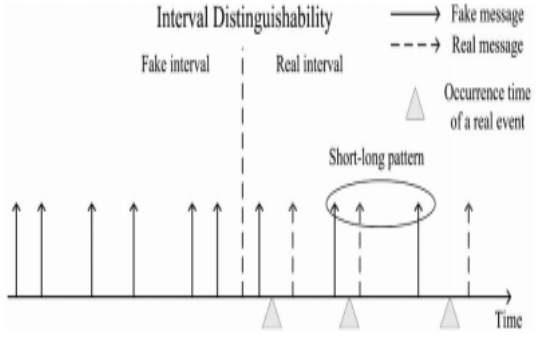

Fig 1.2 Distinguishability level Diagram

D. SEQUENTIAL PROBABILITY RATIO TEST

The enhanced Sequential Probability Ratio Test (SPRT) which is a statistical hypothesis testing. SPRT has been proven to be the best mechanism in terms of the average number of observations that are required to reach a decision among all sequential and non-sequential test processes. SPRT can be thought of as one dimensional random walk with lower and upper limits.

Before the random walk starts, null and alternate hypotheses are defined in such a way that the null one is associated with the lower limit and the alternate one is associated with the upper limit. A random walk starts from a point between two limits and moves toward the lower or upper limit in accordance with each observation.

If the walk reaches or exceeds the lower or upper limit, it terminates and the null or alternate hypothesis is selected, respectively. I believe that SPRT is well suited for tackling the mobile replica detection problem in the sense that I can construct a random walk with two limits in such a way that each walk is determined by the observed speed of a mobile node; the lower and upper limits are properly configured to be associated with the shortfall and excess of the maximum speed of the mobile node, respectively.

The main idea of the proposed scheme is to use sequential hypothesis testing to detect suspect regions in which compromised nodes are likely placed. In these suspect regions, nodes perform software attestation, leading to the detection and revocation of the compromised nodes. Through analysis and simulation, it is shown that the proposed scheme provides effective and robust compromised sensor node detection capability with little overhead.

A mobile replica node u_0 is defined as a node having the same ID and secret keying materials as a mobile node u. An adversary creates replica node u_0 as follows: He first compromises node u and extracts all secret keying materials from it. During the base station collecting all the nodes' location information, the attacker node sends its id (the attacker node) as id of mobile node 'u' (the affected node). Now the goal is to detect the fact that both u and u_0 operate as separate entities with the same identity and keys.

Algorithm process for enhanced SPRT:

DECLARATION:n=0,w_n=0
INPUT: location information L and time information T
OUTPUT: accept the hypothesis H_0 or H_1
curr_loc=L
curr_time=T
if$n$>0 then
    compute$T_0(n)$ and $T_1(n)$
    compute speed 0 from curr_loc and prev_loc, curr_time and prev_time
    if 0>V_{max} then
        w_n=w_n+1
    end if

ifw_n>=$T_1(n)$ then
Accepts the hypothesis $h_1$and terminate the test
end if
ifw_n<=$T_0(n)$ then
initialize$n$ and $w_n$to 0 and accepts the hypothesis H_0
return;
end if
end if
n=n+1
prev_loc=curr_loc
prev_time=curr_time

E. ALGORITHM STEPS IN PROJECT

- Create a network of 'n' nodes and save the information in the database table.
- Draw the network with the available node information.
- Random walk procedure is worked out so that the nodes' mobility is carried out by just moving its location with 'n' pixels below (the given speed) in both x and y direction. For example, if the speed is given as 10 units, then a random value below 10 is chosen, and the node is moved in x or y direction. This is carried out for all nodes. For simulation, the timer is set to 5 seconds. So once each 5 seconds, all the nodes are moved within the given speed horizontally or vertically.
- The nodes are sending their location to their neighbor nodes. The node is treated as neighbor to one, if it is within the given pixel units. For example, the unit is given as 50, then a node with left position in the space with 150 x value and another node with 180 x value is treated as neighbor nodes. This is applicable to y axis also. So in the rectangular area of 50 units (side), when the two nodes fall inside, then they are treated as neighbor nodes.
- The nodes are updating their location information once in 10 seconds. The arrow lines are drawn during the animation such that from all nodes, the line is drawn to the base station. The area located at left bottom corner of the drawing space in the form.
- Replica Attack: When a button is clicked, a node is chosen randomly which behaves as attacker node; a node is chosen randomly which behaves as affected node. The attacker node through sends the current location information, it sends its id as the affected node. So the base station receives updates with two ids at single update. Now, the base station needs to identify which node is correct and which is attacker.
- If two nodes send same id, then the base station, collects the previous location information of the same id. Any one of the entry will have wrong previous location. At the same time, the neighbor nodes location data is also used such that, the affected nodes neighbors update correct location of suspected id whether the attacker nodes neighbor nodes update wrong location and the attacker node will be identified.
- Then the node is revoked from the network.

F. TECHNIQUES TO DETECT COMPROMISED NODES IN ZONES

Reputation-based trust management schemes do not stop compromised nodes doing malicious activities in the network. Also, the existing schemes based on software attestation require each sensor to be periodically attested because it cannot be predicted when attacker compromises sensors. The periodic attestation of individual nodes will incur large overhead in terms computation and communication overhead.

To mitigate the limitations of both approaches, a zone-based node compromise detection scheme is proposed which facilitates node compromise detection and revocation by leveraging zone trust information. Specifically, the network is divided into a set of zones, establish trust per zone, and detect untrustworthy zones inaccordance with zone trust values.

G. PROTOCOL OPERATION

The proposed protocol to find the compromised zones proceeds in three phases:

1) Phase I:

Zone Discovery and Trust Aggregator Selection: After deployment, every sensor node u finds out its location and determines the zone to which it belongs. This zone is called the home zone. From u 's point of view, other zones are called as the foreign zones. Node u discovers every other node residing in the same zone. After the zone discovery process, the Trust Aggregator (TA) is selected in a round robin manner.

2) Phase II:

Trust Formation and Forwarding: For each time slot T i , each node u in zone Z computes neighborhood-trust that is defined in accordance with the difference between the probability distributions of the information generated by u and the information sent to u by u 's neighboring nodes in zone Z

.

3) Phase III:

Detection and Revocation: Upon receiving a zone-trust report from a TA in zone Z , the base station verifies the authenticity of TA's report with the secret shared key between TA and itself and discards the report if it is not authentic. The base station also maintains a record per TA associating each TA's ID with its home zone. This prevents compromised TAs from claiming multiple home zones.

IV.CONCLUSION

This paper proposed to use received signal strength-based spatial correlation, a physical property associated with each wireless device that is hard to falsify and not reliant on cryptography as the basis for detecting spoofing attacks in wireless networks. It provided theoretical analysis of using the spatial correlation of RSS inherited from wireless nodes for attack detection. It derived the test statistic based on the cluster analysis of RSS readings. The approach can both detects the presence of attacks as well as determine the number of adversaries, spoofing the same node identity, so that we can localize any number of attackers and eliminate them. In addition, a zone-based node compromise detection scheme is proposed using the Sequential Probability Ratio Test (SPRT). Furthermore, several possible attacks are described against the proposed scheme and proposed counter-measures against these attacks. In addition, a zone-based node compromise detection scheme is proposed using the Chronological Likelihood Fraction Test (CLFT). The experimental results show that the scheme quickly detects untrustworthy zones with a small number of zone-trust reports.

REFERENCES

[1] B. Alomair, A. Clark, J. Cuellar, and R. Poovendran, "On Source Anonymity in Wireless Sensor Networks," Proc. IEEE/IFIP 40th Int'l Conf. Dependable Systems and Networks (DSN '10), 2010.

[2] K. Mehta, D. Liu, and M. Wright, "Location Privacy in Sensor Networks Against a Global Eavesdropper," in ICNP 2007. IEEE International Conference on Network Protocols. , 2007.

[3] B. Alomair, A. Clark, J. Cuellar, and R. Poovendran, "Statistical Framework for Source Anonymity in Sensor Networks," Proc. IEEE GlobeCom, 2010.

[4] P. Kamat, Y. Zhang, W. Trappe, and C. Ozturk, "Enhanc-ing Source-Location Privacy in Sensor Network Routing," ICDCS 2005. The 25th IEEE International Conference on Distributed Computing Systems.

[5] B. Hoh and M. Gruteser, "Protecting Location Privacy Through Path Confusion," in SecureComm 2005. First Inter-national Conference on Security and Privacy for Emerging Areas in Communications Networks., 2005.

[6] Y. Ouyang, Z. Le, G. Chen, J. Ford, F. Makedon, and U. Lowell, "Entrapping Adversaries for Source Protection in Sensor Networks," in Proceedings of the 2006 IEEE International Symposium on World of Wireless, Mobile and Multimedia Networks, 2006.

[7] K. Mehta, D. Liu, and M. Wright, "Location Privacy in Sensor Networks Against a Global Eavesdropper," in ICNP 2007. IEEE International Conference on Network Protocols., 2007.

[8] M. Shao, Y. Yang, S. Zhu, and G. Cao, "Towards Sta-tistically Strong Source Anonymity for Sensor Networks," INFOCOM 2008. The 27th IEEE Conference on Computer Communications., 2008.

[9] Y. Yang, M. Shao, S. Zhu, B. Urgaonkar, and G. Cao, "To-wards event source unobservability with minimum network traffic in sensor networks," in Proceedings of the first ACM conference on Wireless network security, 2008.

[10] N. Li, N. Zhang, S. Das, and B. Thuraisingham,"Privacy preservation in wireless sensor networks: A state-of-the-art survey," Ad Hoc Networks, 2009.