ISSN: 2348-2079

Volume-11 Issue-2

International Journal of Intellectual Advancements and Research in Engineering Computations

Privacy-Aware and Secure Proof of Wireless Sensor Networks using Sequential Probability Ratio Test

K. Keerthana*, Dr. B.S. Deepapriya

Scholar, Department of Computer Science and Engineering, Erode Sengunthar Engineering College, Perunthurai, Erode – 638057, Tamilnadu, India
Assistant Professor, Department of Computer Science and Engineering, Erode Sengunthar Engineering College, Perunthurai, Erode – 638057, Tamilnadu, India

Corresponding Author: K. Keerthana
Email: keerthanaesc@gmail.com

ABSTRACT

Wireless Sensor Networks (WSNs) are vulnerable to various security threats, making it crucial to ensure their privacy and security. In this paper, we propose a Privacy-Aware and Secure Proof of WSN using Sequential Probability Ratio Test (SPRT) to detect intrusions and ensure the privacy of the data. The Existing method uses SPRT, a statistical test that allows for the detection of changes in the data while minimizing the number of false alarms. The proposed system is designed to be lightweight and energy-efficient, making it suitable for WSNs. The system is evaluated using extensive simulations, and the results demonstrate its effectiveness in detecting intrusions while maintaining a low false alarm rate. The proposed system is a promising approach for enhancing the security and privacy of WSNs, and it can be used in a variety of applications, such as monitoring environmental conditions, industrial process control, and home automation.

The proposed method aims to ensure the integrity of the data collected by the WSN while preserving the privacy of the users. The SPRT is a statistical hypothesis testing technique that can be used to detect anomalous behavior in the data collected by the WSN. The proposed method uses a two-level SPRT scheme to detect malicious attacks and ensure that the data collected by the WSN is trustworthy. Simulation results show that the proposed method is effective in detecting attacks while maintaining the privacy of the users.

The SPRT algorithm is used to detect and reject malicious data injections from adversaries, which can significantly improve the accuracy and reliability of the sensor readings. Furthermore, the proposed scheme incorporates a privacy-preserving mechanism to protect sensitive information from unauthorized access. Experimental results demonstrate that the proposed PAS-POW using SPRT outperforms existing approaches in terms of security and privacy while achieving a high detection rate and low false alarm rate.

Keywords: Wireless Sensor Networks, Sequential Probability Ratio Test, Malicious Attacks

INTRODUCTION

Wireless Sensor Networks (WSNs) have gained significant attention due to their widespread use in various applications such as environmental monitoring, healthcare, and military operations. However, the deployment of WSNs raises significant concerns about data privacy and security. In a WSN, the sensor nodes collect data from the environment and transmit it to the sink node for processing. The sensor data is often sensitive and confidential, and any unauthorized access to this data can lead to severe consequences.

To ensure the integrity and confidentiality of the data collected by WSNs, many security mechanisms have been proposed in the literature. However, most of these approaches focus only on one aspect of security, such as encryption or authentication, while neglecting other crucial aspects such as data integrity and privacy. Moreover, the existing solutions often suffer from high computational complexity, which can significantly affect the efficiency of the network.

WSNs are vulnerable to various attacks, including data tampering, eavesdropping, and node compromise, which can compromise the integrity and confidentiality of the collected

data. To address these issues, several solutions have been proposed to ensure the security and privacy of WSNs.

A new set of security challenges arises in sensor networks due to the act that current sensor nodes lack hardware support for tamper-resistance and are often deployed in unattended environments where they are vulnerable to capture and compromise by an adversary. A serious consequence of node compromise is that once an adversary has obtained the credentials of a sensor node, it can surreptitiously insert replicas of that node at strategic locations within the network. These replicas can be used to launch a variety of insidious and hard-to-detect attacks on the sensor application and the underlying networking protocols. This type of attack is called a node replication attack.

In a centralized approach for detecting node replication, when a new node joins the network, it broadcasts a signed message (referred to as a location claim) containing its location and identity to its neighbors. One or more of its neighbors then forward this location claim to a central trusted party (e.g., the base station). With location information for all the nodes in the network, the central party can easily detect any pair of nodes with the same identity but at different locations. Like all centralized approaches, however, this solution is vulnerable to a single-of-point failure. If the base station is compromised or the path to the base station is blocked, adversaries can add an arbitrary number of replicas into the network without being detected..

we propose a Privacy-Aware and Secure Proof of WSN (PAS-POW) using the Sequential Probability Ratio Test (SPRT) algorithm. Our scheme aims to address the privacy and security concerns of WSNs while maintaining their efficiency. The SPRT algorithm is used to detect and reject malicious data injections from adversaries, which can significantly improve the accuracy and reliability of the sensor readings. Additionally, we incorporate a privacy-preserving mechanism to protect sensitive information from unauthorized access.

EXISTING SYSTEM

A straightforward solution to stop replica node attacks is to prevent the adversary from extracting secret key materials from mobile nodes by equipping them with tamper-resistant hardware. We might expect such measures to be implemented in mobile nodes with security-critical missions. However, although tamper-resistant hardware can make it significantly harder and more time-consuming to extract keying materials from captured nodes, it may still be possible to bypass tamper resistance for a small number of nodes given enough time and attacker expertise.

Since the adversary can generate many replicas from a single captured node, this means that replica attacks are even more dangerous when compared with the possibility of compromising many nodes. We thus believe that it is very important to develop software-based countermeasures to defend mobile sensor networks against replica node attacks.

The primary method used by these schemes is to have nodes report location claims that identify their positions and for other nodes to attempt to detect conflicting reports that signal one node in multiple locations. However, since this approach requires fixed node locations, it cannot be used when nodes are expected to move. Thus, our challenge is to design an effective, fast, and robust replica detection scheme specifically for mobile sensor networks.

DISADVANTAGES

Since the adversary can generate many replicas from a single captured node, this means that replica attacks are even more dangerous when compared with the possibility of compromising many nodes.

We thus believe that it is very important to develop software-based countermeasures to defend mobile sensor networks against replica node attacks.

The primary method used by these schemes is to have nodes report location claims that identify their positions and for other nodes to attempt to detect conflicting reports that signal one node in multiple locations.

However, since this approach requires fixed node locations, it cannot be used when nodes are expected to move. Thus, our challenge is to design an effective, fast, and robust replica detection scheme specifically for mobile sensor networks.

PROPOSED SYSTEM

In this Project, we propose a novel mobile replica detection scheme based on the Sequential Probability Ratio Test (SPRT). We use the fact that an uncompromised mobile node should never move at speeds in excess of the system-configured maximum speed. As a result, a benign mobile sensor node's measured speed will nearly always be less than the system-configured maximum speed as long as we employ a speed measurement system with a low error rate.

On the other hand, replica nodes are in two or more places at the same time. This makes it appear as if the replicated node is moving much faster than any of the benign nodes, and thus the replica nodes' measured speeds will often be over the system-configured maximum speed. Accordingly, if we observe that a mobile node's measured speed is over the system-configured maximum speed, it is then highly likely that at least two nodes with the same identity are present in the network.

If the system decides that a node has been replicated based on a single observation of a node moving faster than it should, we might get many false positives because of errors in speed measurement. Raising the speed threshold or other simple ways of compensating can lead to high false negative rates. To minimize these false positives and false negatives, we apply the SPRT, a hypothesis testing method that can make decisions quickly and accurately.

We perform the SPRT on every mobile node using a null hypothesis that the mobile node has not been replicated and an alternate hypothesis that it has been replicated. In using the SPRT, the occurrence of a speed that is less than or exceeds the system-configured maximum speed will lead to acceptance of the null or alternate hypotheses, respectively. Once the alternate hypothesis is accepted, the replica nodes will be revoked from the network. We validate the effectiveness, efficiency, and robustness of our scheme through analysis and simulation experiments.

Specifically, we find that the main attack against the SPRT-based scheme is when replica nodes fail to provide signed location and time information for speed measurement.

To overcome this attack, we employ a quarantine defense technique to block the noncompliant nodes. We then study this technique in two ways.

First, we show through quarantine analysis that the amount of time, during a given time slot, that the replicas can impact the network is very limited.

Second, we provide a detailed game-theoretic analysis that shows the limits of any attacker strategy over any number of time slots. Specifically, we formulate a two-player game to model the interaction between the attacker and the defender, derive the optimal attack and defense strategies, and show that the attacker's gain is greatly limited when the attacker and the defender follow their respective optimal strategies. We provide analyses of the number of speed measurements needed to make replica detection decisions, which we show is quite low, and the amount of overhead incurred by running the protocol.

In particular, we consider two types of replicas for performance evaluation: mobile and static. In case of mobile replicas, we investigate how replica mobility affects the detection capability of our scheme. In case of static (immobile) replicas, the attacker keeps his replica nodes close together and immobile to lessen the chance of speed-based detection. An exploration of the static replica case is useful since this case represents the worst case for detection, and thus we can see how our scheme works in the worst case. The simulation results of both cases show that this scheme very quickly detects mobile replicas with low false positive and negative rates.

ADVANTAGES

The occurrence of a speed that is less than or exceeds the system-configured maximum speed will lead to acceptance of the null or alternate hypotheses, respectively. Once the alternate hypothesis is accepted, the replica nodes will be revoked from the network. We validate the effectiveness, efficiency, and robustness of our scheme through analysis and simulation experiments.

ARCHITECTURE DIAGRAM

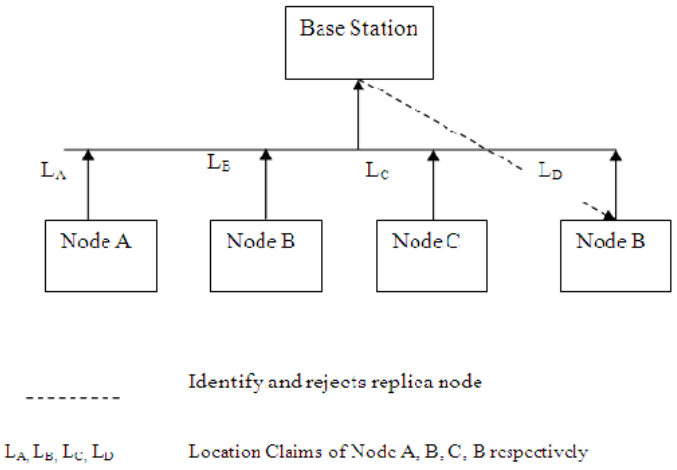


Fig 1: Architecture Diagram

MODULES

1. Network Model
2. Attacker Model
3. Sequential Probability Ratio Test
4. Claim Generation and Forwarding

MODULES DESCRIPTION

1. Network Model

We consider a two-dimensional mobile sensor network where sensor nodes freely roam throughout the network. We assume that every mobile sensor node's movement is physically limited by the system -configure d maximum speed, V_{max}. We also assume that all direct communication links between sensor nodes are bidirectional. This communication model is common in the current generation of sensor networks. We assume that every mobile sensor node is capable of obtaining its location information and also verifying the locations of its neighboring nodes.

This can be implemented by employing secure localization methods. We assume that the clocks of all nodes are loosely synchronized. This can be achieved with the help of secure time synchronization protocols. We also assume that the nodes in the mobile sensor network communicate with a base station. The base station may be static or mobile, although we focus on a static base station for our simulations, as long as the nodes have a way to communicate reliably to the base station on a regular basis.

2. Attacker Model

We assume that an adversary may compromise and fully control a subset of the sensor nodes, enabling him to mount various kinds of attacks. For instance, he can inject false data packets into the network and disrupt local control protocols such as localization, time synchronizations, and route discovery process. Furthermore, he can launch denial-of-service attacks by jamming the signals from benign nodes.

We place some limits on the ability of the adversary to compromise nodes. We note that if the adversary can compromise major fraction nodes of the network, he will not need nor benefit much from the deployment of replicas. To amplify his effectiveness, the adversary can also launch a replica node attack, which is the subject of our investigation. We assume that the adversary can produce many replica nodes and that they will be accepted as a legitimate part of the network.

We also assume that the attacker attempts to employ as many replicas of one or more compromised sensor nodes in

the network as will be effective for his attacks. The attacker can allow his replica nodes to randomly move or he could move his replica nodes in different patterns in an attempt to frustrate our proposed scheme.

We also assume that the base station is a trusted entity. This is a reasonable assumption in mobile sensor net-works, because the network operator collects all sensor data and can typically control the node s' operation through the base station. Thus, the basic mission of the sensor network is already completely undermined if the base station is compromised.

3. Sequential Probability Ratio Test

Fortunately, mobility provides us with a clue to help resolve the mobile replica detection problem. Specifically, a benign mobile sensor node should never move faster than the system-configured maximum speed, Vmax. As a result, a benign mobile sensor node's measured speed will appear to be at most Vmax as long as we employ a speed measurement system with a low rate of error.

Replica nodes will appear to move much faster than benign nodes and thus their measured speeds will likely be over Vmax because they need to be at two (or more) different places at once. Accordingly, if the mobile node's measured speed exceeds Vmax, it is then highly likely that at least two nodes with the same identity are present in the network.

We propose a mobile replica detection scheme by leveraging this intuition. Our scheme is based on the Sequential Probability Ratio Test which is a statistical decision process. The SPRT can be thought of as one-dimensional random walk with the lower and upper limits. Before the random walk starts, null and alternate hypotheses are defined in such a way that the null hypothesis is associated with the lower limit while 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.

We believe that the SPRT is well suited for tackling the mobile replica detection problem since we 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 can be configured to be associated with speeds less than and in excess of Vmax, respectively.

We apply the SPRT to the mobile replica detection problem as follows: Each time a mobile sensor node moves to a new location, each of its neighbors asks for a signed claim containing its location and time information and decides probabilistically whether to forward the received claim to the base station. The base station computes the speed from every two consecutive claims of a mobile node and performs the SPRT by considering speed as an observed sample. Each time the mobile node's speed exceeds (respectively, remains below) Vmax, it will expedite the random walk to hit or cross the upper (respectively, lower) limit and thus lead to the base station accepting the alternate (respectively, null) hypothesis that the mobile node has been (respectively, not been) replicated. Once the base station decides that a mobile node has been replicated, it revokes the replica nodes from the network.

4. Claim Generation and Forwarding

Each time a mobile sensor node u moves to a new location, it first discovers its location Lu and then discovers its set of neighboring nodes, N (u).Every neighboring node V€ N(u) asks node u for an authenticated location claim by sending its current time T to node u.

Upon receiving T, node u checks whether T is valid or not. If |T`-T |> ∞+€, where T` is the claim receipt time at u, ∞ is the estimated transmission delay of claim, and € is a maximum error in time synchronization, then node u will ignore the request. Otherwise, u generates location claim Cu = {u||Lu||T_k||S_ig_u} and sends it to V, where S_ig_u is the signature over the tuple (u;Lu;T) generated using node u's private key. If u denies the claim requests, or if its claim contains invalid time information or fails to authenticate, then u will be removed from NðvÞ.

Also, if u claims a location Lu such that the distance between Lv and Lu is larger than the assumed signal range of v, then it will be removed from NðvÞ. Once the above filtering process is passed, each neighbor v of node u forwards u's claim to the base station with probability p. regarding errors in the measurement of time and location, we can consider both random and systematic errors. Since speed is measured based on location and time, the errors can come from either measurement.

We note that the time of each claim is measured and verified by the requesting node, rather than the measured node. Since claim verification and forwarding is done probabilistically, the chance of having two verified and forwarded claims from the same requesting node is low.

Thus, systematic time measurement error at the requesting node is likely to result in independent errors between each location claim for the nodes being measured. Systematic location measurement error means that the measurements are not independent. However, if we assume that the measurement error is consistent and biased in one direction, then the speed of a node will be measured accurately in most cases.

Random location measurement errors are more likely to lead to errors in speed measurement. Thus, for our system, we treat error from one claim to the next as random and independent for the measurement of nodes' speeds.

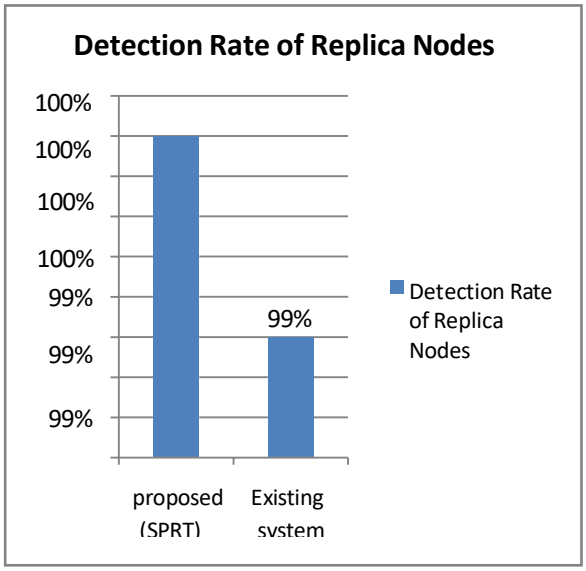
RESULT AND DISCUSSION

The result and discussion chapter describe detection of mobile replica nodes using sequential probability ratio test. Includes experimental setup, experimental results for existing detection schemes based on the performance with the proposed detection techniques based on reviews and discussion. The metrics used for the proposed work are detection rate, mobility rate and overhead.

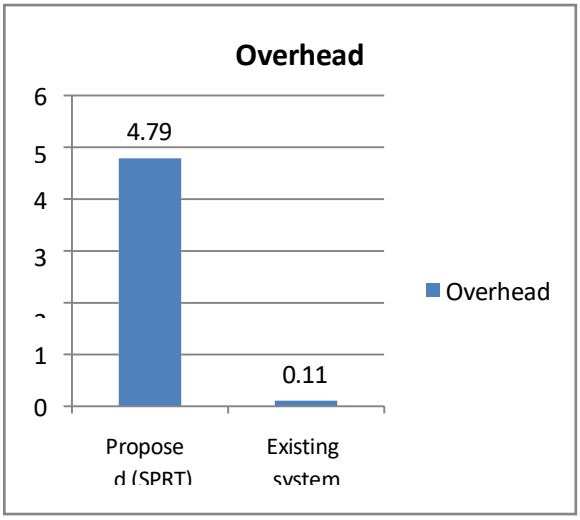
Implementation Details

During the implementation, location ID is provided to each mobile sensor node and every mobile sensor node u generates location claim Cu = {u||Lu||T||Sigu} and sends it to a neighboring node v, where u, is the node identity, Lu is the Location, T is the Time and Sigu is the signature generated by node u's private key. Each time a mobile sensor node u moves to a new location, it first discovers its location Lu. Base station receive location claim from the mobile sensor nodes. Upon receiving a location claim, the

base station verifies the authenticity of the claim with the public key of node u and discards the claim if it is not authentic. Threshold value for the maximum velocity of the mobile sensor node is given in base station. When a mobile sensor node moves from one location L1 to another location L2, the Euclidean distance is calculated between L1 and L2 (L2-L1). Similarly the time for the above location movement is measured using (T2-T1). Speed for a mobile sensor node is calculated using Speed S= (L2-L1) / (T2-T1).



a) Graph of existing system and proposed SPRT regarding detection rate (replica nodes).



b) Graph of existing system and proposed SPRT regarding overhead.

CONCLUSION

A secure and privacy-aware scheme for LP generation and verification. The proposed scheme has a decentralized architecture suitable for *ad hoc* applications in which mobile users generate LPs for each other. To address terrorist frauds, we developed a DB protocol P-TREAD, that is, a private version of TREAD, and integrated it into PASPORT. Using P-TREAD, a dishonest prover who established a prover-prover collusion with an adversary can easily be impersonated by the adversary later. Thus, no logical user takes such a risk by initiating a prover–prover collusion. Furthermore, we employed a witness selection mechanism to address the prover–witness collusions. Using the proposed mechanism, available witnesses are randomly assigned to requesting provers by the verifier.

FUTURE ENHANCEMENT

The proposed Privacy-Aware and Secure Proof of WSN (PAS-POW) using Sequential Probability Ratio Test (SPRT) algorithm is a promising solution for ensuring the privacy and security of WSNs. However, there is always room for improvement and future enhancements. Here are some possible avenues for future research:

Multi-level security: The proposed PAS-POW using SPRT provides a basic level of security for WSNs. Future research can explore the integration of multi-level security mechanisms that provide different levels of protection for different types of data or nodes in the network.

Energy efficiency: The proposed PAS-POW using SPRT may require a significant amount of energy for the data transmission and processing. Future research can explore

ways to optimize the energy consumption of the network without compromising its security and privacy.

Scalability: The proposed scheme has been evaluated in a small-scale environment. Future research can explore the scalability of the scheme for large-scale WSNs and real-world scenarios.

Integration with block chain technology: The integration of block chain technology can provide an additional layer of security and privacy for WSNs. By using a decentralized and tamper-proof ledger, block chain can prevent malicious entities from altering the data or compromising the integrity of the network.

REFERENCES

1. Asuquo P, Cruickshank H, Morley J, Ogah CPA, Lei A, Hathal W et al. Security and privacy in location-based services for vehicular and mobile communications: an overview, challenges, and countermeasures. IEEE Internet Things J. Dec 2018;5(6):4778-802. doi: 10.1109/JIOT.2018.2820039.
2. Vo QD, De P. A survey of fingerprint-based outdoor localization. IEEE Commun Surv Tuts. 2016;18(1):491-506, 1st Quart.. doi: 10.1109/COMST.2015.2448632.
3. Gupta R, Rao UP. An exploration to location–based service and its privacy preserving techniques: A survey. Wireless Pers Commun. 2017;96(2):1973-2007. doi: 10.1007/s11277-017-4284-2.
4. Global location–based services market; 2018-2023. [accessed: Jul 20, 2019] [online]. Available from: https://www.businesswire.com/news/home/20180927005490/en/Global–Location-based-Services-Market-2018-2023-Projected-Grow.
5. Zheng Y, Li M, Lou W, Hou YT. Location based handshake and private proximity test with location tags. IEEE Trans Depend Sec Comput. Jul/Aug 2017;14(4):406-19. doi: 10.1109/TDSC.2015.2472529.