A novel ARED Protocol for detection of clone attacks in wireless sensor networks

A.Divia lakshmi [1], N.Sudha [2]

[1] *Research scholar,* [2] *Assistant professor, Department of Computer Science, Bishop Appaswamy College, Coimbatore.*
adivialakshmi@gmail.com[1] , msudhamuruganathan@gmail.com[2]

Abstract

Objectives: To develop a new technique that avoids the clone attack without affecting the performance of the wireless network.
Methods: An Authentic, Randomized, Efficient, Distributed (ARED) protocol is introduced for detect the clone attacks from wireless sensor networks. This method does not require high memory and energy like other methods but provides high authentic context. The attractive feature of this method is that it detects the clones even before it is introduced into the network by the adversary. It provides continuous communication to the end users while detecting the clone attacks. Thus the system can be highly secured and can be used for the real time data acquisition systems.
Findings: The proposed method achieves high performance in terms of end to end delay, packet delivery ratio and Throughput.
Application/Improvements: The proposed detection mechanism is done by using Authentic, Randomized, Efficient, Distributed (ARED) protocol. It achieves high detection performance compared to the existing system.

Keyword: Mobile sensor node, Memory, Private Key, clone attacks.

1. Introduction

Wireless sensor networks are having spatially dispersed sensors which are used to monitor the environmental conditions such as temperature, humidity and etc [1][2][3]. The sensed informations are passed through the network to a base station. The base station is answerable for information collection, analysis and it maintains the sensor nodes in wireless sensor networks. Protecting sensor networks from different attacks such as black hole attack [4] [5], Sybil attack [6] and replication attack is a major problem. In that situation attacker may capture the sensor nodes, and then embed the fake data into them. This will be affects the whole network operation.

For instance, an adversary could eavesdrop all network communications; the adversary captured sensors nodes and replicated them in the network to produce different malicious activities. This is known as clone attack. There are several methods are proposed for detect the replica node in static sensor network. This type of detection scheme is to have nodes report location claims that identify their position and attempt to detect conflicting reports that signal one node in multiple locations. However it is difficult when the sensor nodes are in moment.

Richard Brookset.al proposed a new clone node detection mechanism which is based on the Random Key Pre-distribution**.** Cloned nodes could collude to use their keys differently from legitimate nodes. If these keys are detected, they may then switch to other keys. This approach would make clones easier to detect, since the keys that they collude to use would be used even more often than normally. In any case whenever a node authenticates itself using a key, such information should be analyzed to guard against the insertion of a clone [7] . However it is unable to find consecutive clones as it lacks storage informations.

Heesook Choi et.al [8] introduced a SET scheme which is used for detect the clone attacks. It five component. There are exclusive subset construction, authentication of subset covering, distributed set computation and interleaved authentication on subset trees, and verifiable random selection. At first, the unit subsets are formed among one-

hop neighbors in the wireless sensor network. It offers authentication to nodes' subset membership. To calculate non overlapped set operations, the SET scheme use tree structure. Finally the Randomization scheme is used for further make the exclusive subset and tree formation unpredictable to an adversary. However it does not suitable for mobile sensor networks.

Yingpei Zeng et.al [9] proposed a Random-Walk Based Approach which is used for detect Clone Attacks. To overcome the communication overhead**,** the proposed system introduced two protocols. There are RAndom WaLk (RAWL) and Table-assisted RAndom WaLk (TRAWL) protocols. The RAWL protocol starts numerous walk arbitrarily in the network .And then selects passed nodes as the witness nodes**.** It detects the replication node with huge probability. To reduce the memory cost RAWL protocol is introduced which and insert a trace table at each node. However it has huge complexity.

The proposed a Sequential Probability Ratio Test for detects the clone nodes with high speed. Initially the network begins from the node 0. Then the node Informations like location and time are gathered. The Informations of the initial node are considered primarily. Then the time is set and the distance traveled by the node in that time is noted. This data is used to compute the speed of the node. It is compared with the maximum speed. If the node speed is more than the maximum speed then it is marked as clone. Otherwise the node is left for communication and the process is continued for the next node.

2. Materials and Methods

2.1. Network model

An undirected graph G (V, E) where the set of vertices V represent the mobile sensor nodes in the network and E represents set of edges in the graph which represents the physical or logical links between the mobile sensor nodes. Let N denote a network of m number of nodes, $N_1, N_2, \dots N_m$ and let D denote a collection of n data items $d_1, d_2, \dots d_n$ distributed in the network. Before deployment, each sensor nodes obtains secret keying materials for creating digital signatures. Every mobile sensor nodes in a network is able to find out its location information and confirm its neighboring nodes location.

2.2. Claim Generation and Forwarding

After the initialization mobile sensor nodes in network**,** Every time a mobile sensor node *u* moves to a new location, the primary function is find out its location L_u and then identify a set of neighboring nodes *N*(*u*). For genuine location claim*,* every neighboring node sends its present time T to node u. Then node u verifies the receiving present time is valid or not.

$$| T' - T | > \delta + \varepsilon$$

Where,

T' – Claim receipt time at u
δ - Evaluated transmission delay of claim
ε - Maximum error
If condition is true the mobile sensor node u rejects the request. Otherwise node u creates location claim. The location claim is computed by following equation,

$$C_u = \{ u || L_u || T || sig_u \}$$

Where,
V- Neighbouring node
sig_u- Signature of node u's private key
L_u – Location of node u

This location claim is send to neighboring node v. The mobile sensor node u is removed from N (v) while its claim not succeeds to authenticate. And also, if the distance between neighbouring node location and mobile sensor node u location is greater than the signal range of v, it may eliminate from N (v). The neighbour node of u broadcast mobile sensor node u's claim to base station with probability p if the above conditions are true.

2.3. Detection and Revocation

The neighbour nodes are broadcast the location claim to base station. The base station checks the authenticity of the claim with the public key of node. If the authenticity of the claim is false it will be eliminated. Let we assume$C_u^1, C_u^2, \ldots,$. From C_u^i the base station take out the L_u^i and T^i.
Measured speed is computed by the following equation,

$$O_i = \frac{d_i}{|T_i - T_{i-1}|}$$

Where,
$O_i -$ Measure speed
$d_i -$ Euclidean distance from location L_u^{i-1} to L_u^i
Bernoulli random variable that is defined

$$S_i = \begin{cases} 0 & \text{if } o_i \le V_{max} \\ 1 & \text{if } o_i > V_{max} \end{cases}$$

Bernoulli distribution success probability is represented as

$$\Pr(Si = 1) = 1 - \Pr(Si = 0) = P_r = (S_i = 1) = 1 - p_r (S_i = 0) = \lambda$$

$\lambda > \lambda'$

If the above condition is true, the mobile sensor node u has been replicated. Otherwise it not been replicated. This replication problem formulated as a hypothesis testing problem. The hypothesis testing trouble taking as one with null and alternate Hypotheses. If $\lambda \le \lambda_0$, hypothesis is observe as an false positive error and if $\lambda \ge \lambda_1$, null hypothesis is regarded as false negative error. The user-configured false positive α' and false negative β' for prevent the decision procedure from these two types of errors. These false positive and false negative errors does not larger than α' and β'.

Let $L\ n$ denote the number of times that *Si* = 1 in the *n* samples. Then we have

$$L\ n = w_n \ln \frac{\lambda_1}{\lambda_0} + (n - w_n) \ln \frac{1-\lambda_1}{1-\lambda_0}$$

Where,

$\lambda_0 = P_r(S_i=1|H_0)$, $\lambda_1 = P_r(S_i=1|H_1)$

λ_0 Should be configured in accordance with the likelihood of the occurrence that benign node's speed exceeds Vmax due to the time synchronization and localization errors. λ_1 Should be configured to consider the likelihood of the occurrence that replica nodes' speeds exceed Vmax.

On the basis of the log-probability ratio L_n, the SPRT for H_0 against H_1 is given as follows:

$L_n \le \ln \frac{\beta'}{1-\alpha'}$: accept H_0 and terminate the process

$L_n \ge \ln \frac{1-\beta'}{\alpha'}$: accept H_1 and terminate the process

$ln \frac{\beta'}{1-\alpha'} < L_n < \frac{1-\beta'}{\alpha'}$: continue the test process with another observation.

2.4. Authentic Randomized Efficient Distributed (ARED) protocol

The proposed ARED protocol provides a authentication to the network as a whole as well as individual nodes. The method initially utilizes a fixed number of nodes so that when a node is cloned the number of nodes exceeds the fixed number. Thus the detection is made. This method makes use of a secret key. The nodes are initially selected randomly from a set of nodes. Then the data is transmitted into the nodes with distributive node table which is similar to hash table that containing the subsequent node informations. As the secret keys are used for transmission the random loops are avoided. The node information's are analyzed and the nodes are checked for any cloned nodes by this table. If the nodes are found normal then they authenticated by a secret key. The probability for clone is checked initially and if there is even a small probability the further analysis are made. The memory and power consumption parameters are checked such that if a clone appears it uses more resources than normal. Hence by this approach the clone attacks are detected even before it is introduced into the network.

2.5. Algorithm

Step1: Initialize N

N-Number of sensor nodes

Step 2: Construct table with Neighbor nodes

Step 3: Assign authentication

Step 4: If P>0

Step 5: probability of clones

Step 6 : Analysis power and memory

Step 7: Check memory

Step 7: If high memory

Step 8: Detect clones

Step 9: Otherwise

Step 10: Go to step 2

Step 11: It continue until non clone nodes in network

3. Experimental result

The existing and proposed methods are evaluated in terms of end to end delay , packet delivery ratio and Throughput.

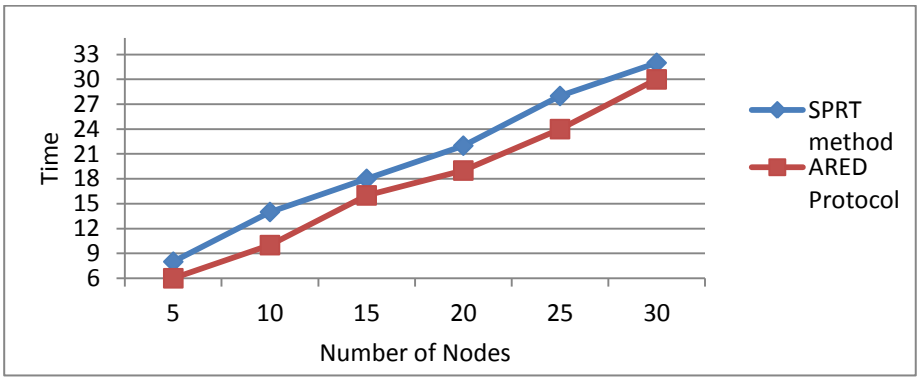
Description of output parameter

3.1 End to end delay

End-to-end delay refers to the time taken for a packet to be transmitted across a network from source to destination.

From the above figure 1 can be proved that the proposed methodology provides better result than the existing approach. In this figure x axis plots the number of nodes and y axis plots the time. The time taken for a packet to be transmitted across a network from source to destination is efficient compare to existing one.

Figure 1. End to end delay



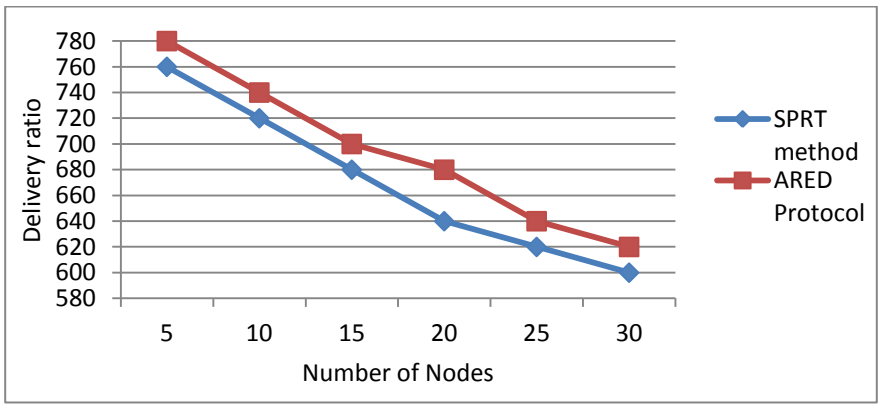
3.2 Packet delivery ratio

It is defined as the ratio of the number of delivered data packet to the destination. This illustrates the level of delivered data to the destination.

$$\frac{\sum Number\ of\ packet\ receive}{\sum Number\ of\ packet\ send}$$

In figure 2, x axis plots the number of nodes and y axis plots the packet delivery ratio. This graph clearly shows that if the number of nodes is increases the packet delivery ratio of the network is decrease. The ratio of the number of delivered data packet to the destination is high compare to the existing one

Figure 2. Packet delivery ratio

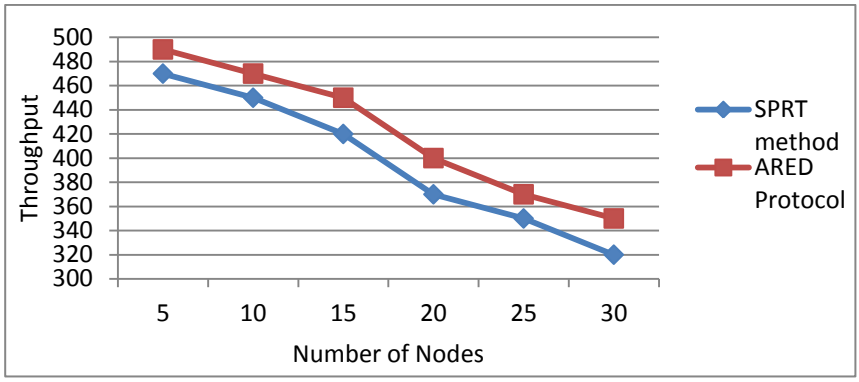


3.3 Through put

Throughput or network throughput is the amount of successful packets delivery over a communication network

From figure 3, x axis plots the number of nodes and y axis plots the Throughput value. This graph clearly shows that if the number of nodes is increases the throughput of the network is decreased. The rate of successful message delivery over a communication channel is high compared to existing one.

Figure 3. Through put



4. Conclusion

A Newly designed Authentic, Randomized, Efficient, and Distributed (ARED) protocol is used for efficiently detect the node replication attack compared to Sequential Probability Ratio Test protocol. The main function of this protocol is detects the clones even before it is introduced into the network by the adversary. ARED protocol detects the clones at the same time it provides continuous communication to users. The experimental results show that the proposed ARED protocol provides high authentic security and also avoids false data compared to the existing methods.

5. References

1. Raghav Sethi, Dr. Raman Chadha. Power resourceful routing for wireless sensor networks (WSN). *International Journal of Core Engineering & Management (IJCEM)*. 2015; 2(2), 89-96.
2. Pankaj Chauhan, Tarun Kumar. Power optimization in wireless sensor network: A perspective. *International Journal of Engineering and Technical Research (IJETR)*. 2015; 3(5), 273-277.
3. K Praveen Kumar Rao, K Kalaiarasi. Data centric routing protocols in wireless sensor networks: A survey. *European Journal of Advances in Engineering and Technology*. 2015; 2(6), 62-69.
4. B.R.Baviskar, V.N.Patil. Black hole attacks prevention in wireless sensor network by multiple base station using of efficient data encryption algorithms. *International Journal of Advent Research in Computer & Electronics*. 2014; 1(2),6-9.
5. B.R.Baviskar, V.N.Patil. Black hole attacks mitigation and prevention in wireless sensor network. *International Journal of Innovative Research in Advanced Engineering (IJIRAE)*. 2014; 1(4), 167-169.
6. T. N. Manjunatha, M. D. Sushma, K. M. Shivakumar. Security concepts and sybil attack detection in wireless sensor networks. *International Journal of Emerging Trends and Technology in Computer Science (IJETTCS)*. 2013; 2,(2), 383-390.
7. Richard Brooks, P. Y. Govindaraju, Matthew Pirretti, N. Vijaykrishnan, Mahmut T. Kandemir. On the detection of clones in sensor networks using random key predistribution. *IEEE transactions on systems, man, and cybernetics—part c: applications and reviews*. 2007; 37(6), 1246-1258.
8. Heesook Choi, Sencun Zhu, Thomas F. La Porta. SET: Detecting node clones in Sensor Networks. 2007.
9. Yingpei Zeng, Jiannong Cao, Shigeng Zhang, Shanqing Guo, Li Xie. Random-walk based approach to detect clone attacks in wireless sensor networks. *IEEE journal on selected areas in communications*.2010; 28(5), 677-691.