Clone Detection for Efficient System in WSN Using AODV

Submitted By
Ms. RupikaYadav
M Tech III Sem
TGPCET, Nagpur

Co-guide
Prof RoshaniTalmale
HOD, CSE
TGPCET, Nagpur

Guide
Prof Vishal Tiwari
Dept. of CSE
TGPCET, Nagpur

***Abstract*—**Wireless sensor networks accommodate a whole lot to thousands of sensor nodes and are wide employed in civilian and security applications. One in every of the intense physical attacks faced by the wireless sensor network is node clone attack. So 2 node clone detection protocols area unit introduced via distributed hash table and arbitrarily directed exploration to detect node clones. The previous primarily based on a hash table value that is already distributed and provides key based facilities like checking and caching to observe node clones. The later one is exploitation probabilistic directed forwarding technique and border determination. The simulation results for storage consumption, communication value and detection chance is completed exploitation NS2 and obtained arbitrarily directed exploration is that the best one having low communication value and storage consumption and has smart detection chance.

***Keywords*—** *Security attack, Base Station, Clone attack, Clone attack detection, Centralized approach, Distributed approach.*

*****

1. INTRODUCTION

1.1 Background

A Wireless sensor Network or WSN is meant to be made from a large variety of sensors and a minimum of one base station. The sensors are autonomous little devices with many constraints just like the battery power, computation capability, communication range and memory. They are also furnished with transceivers to assemble data from its surroundings and pass it on up to a particular base station, wherever the measured parameters may be hold on and offered for the end user.

In most cases, the sensors forming these networks are deployed arbitrarily and left unattended to and are expected to perform their mission properly and with efficiency. As a results of this random readying, the WSN has typically varied degrees of node density on its space. Sensor networks also are energy strained since the individual sensors that the network is created with, are extraordinarily energy-constrained moreover. The communication devices on these sensors are little and have restricted power and range.

Both the most likely distinction of node density among some regions of the network and also the energy constraint of the sensor nodes cause nodes slowly die creating the network less dense. Also it's quite common to deploy WSNs in harsh surroundings, what makes several sensors inoperable or faulty. For that reason, these networks need to be fault-tolerant so the requirement for maintenance is decreased. Usually the network topology is incessantly and dynamically ever-changing, and it's truly not a desired resolution to fill again it by infusing new sensors instead the depleted ones. A true and applicable resolution for this drawback is to implement routing protocols that perform with efficiency and utilizing the less quantity of energy as possible for the communication among nodes.

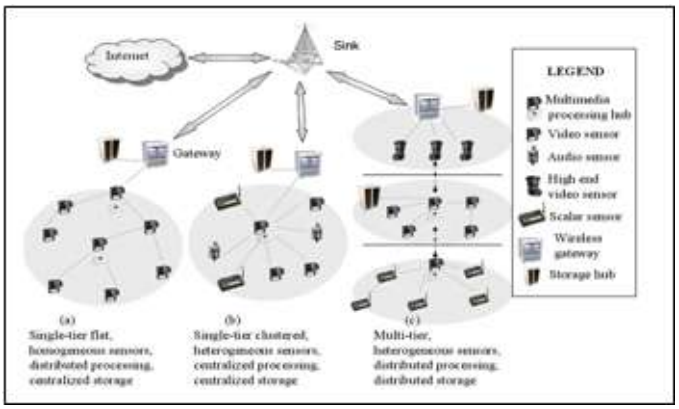


Figure 1: Overview of Wireless Sensor Networks

The WSN consist of two main components:
i. Sensor Nodes, andii. Base Station (Central Gateway).

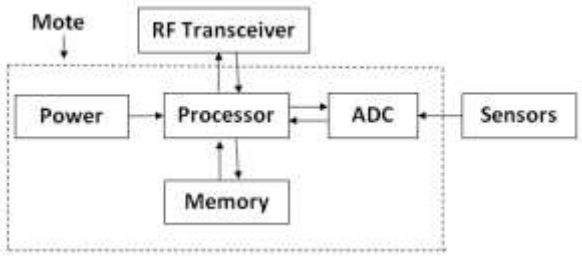


Figure 2: Block diagram of Sensor Node

Sensor nodes

Sensors nodes are generally designed of few sensors and a mote unit as shown in Fig.1.2. A sensor could be a device that senses the data and pass it on to mote. Sensors are generally accustomed measure the changes in physical environmental parameters like temperature, pressure, humidity, sound,

vibration and changes within the health parameter of person e.g. blood pressure level and heartbeat. MEMS primarily based sensor have found sensible use in sensor nodes. A mote consists of processor, memory, battery, A/D converter for connecting to a sensor and a radio transceiver for forming an ad hoc network. A mote and sensor along form a sensor Node. A sensor network could be a wireless ad-hoc network of sensor nodes. Every sensor node will support a multi-hop routing algorithmic rule and performance as forwarder for relaying information packets to a base station.

Base Station

A base station links the sensor network to a different network. It consists of a processor, radio board, antenna and USB interface board. It's preprogrammed with low-power mesh networking code for communication with wireless sensor nodes. Readying of the base station in a very wireless sensor network is incredibly necessary as all the sensor nodes relinquishment their information to the base station for process and higher cognitive process. Energy conservation, coverage of sensing element nodes and reliableness problems are taken care of during readying of base station in sensor network. Typically base stations are assumed static in nature however in some situations they're assumed to be mobile to gather the information from sensor nodes.

1.2 Our contribution

In this paper, besides the clone detection probability, we tend to in addition believe energy consumption and memory storage among the design of clone detection protocol, i.e., an energy- and memory-efficient distributed clone detection protocol with random witness alternative theme in WSNs.Our protocol is applicable to general densely deployed multi-hop WSNs, where adversaries would possibly compromise and clone sensor nodes to launch attacks.

We extend the analytical model by evaluating the required data buffer of ERCD protocol and by together with experimental results to support our theoretical analysis. Energy-Efficient Ring based totally Clone Detection (ERCD) protocol.We find that the ERCD protocol can balance the energy consumption of sensors at totally different locations by distributing the witnesses all over WSNs except non-witness rings, i.e., the adjacent rings round the sink, that should not have witnesses.After that, we tend to acquire the optimum vary of non-witness rings based on the perform of energy consumption. Finally, we tend to derive the expression of the required data buffer by using ERCD protocol, and show that our projected protocol is scalable as a result of the required buffer store depends on the ring size solely.

2. Related Work

Most important security issues, clone attack has attracted people's attention. There are many works that studies clone detection protocols among the literature, which can be classified into two fully different classes, i.e., centralized and distributed clone detection protocols. In centralized protocols, the sink or witnesses typically notice among the middle of each region, and store the personal information of sensors. Once the sink or witnesses receive the private information of the source node, they'll verify whether or not there is a clone attack by examination the private information with its pre-stored records. Normally, centralized clone detection protocols have low overhead and running quality. However, the protection of sensors' private information may not be bonded, as a results of the malicious users can overhang drop the transmission between the sink node and sensors. Moreover, the network time period might even be dramatically reduced since the sensor nodes close to the sink will expend their energy before various nodes. Differ from centralized protocols, in distributed clone detection protocols, a set of witnesses are elite to match with every sensor that stops the transmission between the sink and sensors from being eavesdropped by malicious users.There are three differing kinds of witness selection schemes in distributed clone detection protocols: i) settled choice, ii) random selection, and iii) clone detection protocols like RED choose constant set of witnesses for all sensor nodes. By exploitation settled witness selection, an occasional communication overhead and a high clone detection probability is also achieved. In addition, the required memory device capability of such protocols is very low, that's simply related to the quantity of witnesses whereas not considering network scale and node density. Withal, as a results of the settled characteristic, the mapping perform is also merely obtained and a range of attacks is additionally launched by malicious users. To strengthen the network security, the distributed clone detection protocols with random witness choice, like LSM are planned, that are closely related to our work. In random witness choice, it's robust for malicious users to accumulate the information of witnesses since the witnesses of each sensor are at random generated.

However, the randomness of mapping perform in addition will increase the problem for the source node to attain its witnesses that creates it difficult to realize a high clone detection probability. To form positive the clone detection probability, LSM lets all the nodes inside the route between source and witnesses store the private information of the source node that leads to a high demand of data buffer and energy consumption. Thus, it's essential to confirm the clone detection probability with low energy consumption and required memory device in clone detection protocols with random witness choice approach.

3. Sensor network model

3.1. Setting up Network Model

Our 1st module is putting in the network model. We tend to contemplate a large-scale, consistent sensor network consisting of resource-constrained sensor nodes. Analogous to previous distributed detection approaches; we tend to assume that an identity-based public-key cryptography facility is accessible within the sensor network. Before readying, every legitimate node is allotted a unique ID and a corresponding non-public key by a trusty third party. The general public key of a node is its ID, that is that the essence of an identity-based cryptosystem. Consequently, no node will delude others regarding its identity. Moreover, anyone is ready to verify messages signed by a node exploitation the identity-based key. The source nodes in our drawback formulation serve as storage points that cache the information gathered by different nodes and sporadically transmit to the sink, in response to user queries. Such network architecture is in keeping with the planning of storage centrical sensor networks

3.2. Initialization Process

To activate all nodes starting a new spherical of node clone detection, the instigator uses a broadcast authentication theme to unleash an action message likewise as a monotonously increasing present, a random spherical seed, and an action time. The present is supposed to prevent adversaries from launching a DoS attack by repetition broadcasting action messages.

3.3. Claiming neighbor's information

Upon receiving an action message, a node verifies if the message nowadays is larger than last time being and if the message signature is valid. If every pass, the node updates the present and stores the seed. At the chosen action time, the node operates as an observer that generates a claiming message for each neighbor (examinee) and transmits the message through the overlay network with regard to the claiming probability. Nodes can begin transmitting claiming messages at an identical time, on the opposite hand huge traffic would possibly cause serious interference and degrade the network capability. To alleviate this disadvantage, we would specify a sending amount, throughout that nodes randomly get a transmission time for every claiming message.

3.4. Processing claiming messages

A claiming message are forwarded to its destination node via several Chord intermediate nodes. Exclusively those nodes at intervals the overlay network layer ought to technique a message, whereas various nodes on the trail simply route the message to temporary targets. Algorithm for handling a message is that the kernel of our SCRW. If the rule returns null, then the message has encounter its destination. Otherwise, the message are anon forwarded to succeeding node with the ID that is came back

3.5. Sink Module

The sink is that the aim of contact for users of the sensor network. Anytime the sink receives a problem from a user, it first interprets the question into multiple queries then disseminates the queries to the corresponding mobile relay, that technique the queries supported their data and are available back the question results to the sink. The sink unifies the question results from multiple storage nodes into the last word answer and sends it back to the user.

4. ERCD PROTOCOL

Initially, network region is nearly divided into h adjacent rings, where every ring contains a sufficiently sizable amount of sensor nodes to forward on the ring and also the breadth of every ring is r. To alter the outline, we tend to use hop length to represent the smallest number of hops within the paper. Since we tend to think about a densely deployed WSN, hop length of the net-work is that the quotient of the space from the sink to the sensor at the border of network region over the transmission vary of every sensor, i.e., the space of every hop refers to the transmission vary of sensor nodes. The ERCD protocol starts with a breadth-first search by the sink node to initiate the ring index, and every one neighboring sensors sporadically exchange the relative location and ID data.

Thus, whenever a sensor node establishes a data transmission to others, it has to run the ERCD protocol, i.e., witness selection and legitimacy verification, to verify its legitimacy. In witness selection, a ring index is randomly selected by the mapping function as the witness ring of node a. To help relieve the traffic load in hot spot, the area around the sink cannot be selected by the mapping function. After that, node a sends its private information to the node located in witness ring, and then the node forward the information along the witness ring to form a ring structure. In the legitimacy verification, a verification message of the source node is forwarded to its wit-nesses. The ring index of node O_a^{ω}, denoted Oa, is compared with its witness ring index to determine the next forwarding node. If $O_a^{\omega} > O_a$, , the message will be forwarded to any node located in ring O_a+1 ; otherwise, the message will be forwarded to any node in ring O_a -1. This step can forward the message toward the witness ring of node a. The ERCD protocol repeats above operations until a node, denoted b, located in the witness ring O_a^{ω} is reached. Node b stores the private information of node a and forwards the message to any node located in ring O_a^{ω} within its transmission range, denoted asc. Then, node c stores the information and forwards the message to the noded, where link (c,d) has longest projection on the extension line of the directional link formbook.

The procedure will be repeated until node b reappears in the transmission range. Therefore, the witnesses of node a have a ring structure, consisting of b; c;…b In the legitimacy

verification, node a sends a verification message including its private information following the same path towards the witness ring as in witness selection. To enhance the probability that witnesses can successfully receive the verification message for clone detection, themes-sage will be broadcast when it is very close to the witness ring, namely three-ring broadcasts, i.e., the message will be broadcast in $O_a^\omega - 1, O_a^\omega \; and \; O_a^\omega + 1$ .we prove that the three-ring broadcasts can ensure the network security, i.e., the clone detection probability is one, under the assumption that all witnesses are trustful. To determine whether there exists a clone attack or not, all the verification messages received by witnesses are forwarded to the witness header along the same route in wit-ness selection. The sensor nodes in the transmission route but not located in the witness ring are called the transmitters.

The witness header of the source node a, denoted by Sa and is a sensor located in witness ring O_a^ω , meanwhile it is also in the communication range of the transmitter located in ring index $O_a^\omega - 1 \; or \; O_a^\omega + 1$. The witness header Sa is randomly selected by the transmitter in the neighboring witness ring, i.e., the ring of $O_a^\omega - 1 \; or \; O_a^\omega + 1$. If more than one copies or incorrect copies or expired copies are received by thewitness header, the ERCD protocol will trigger a revocation procedure; if no copy is received from the source node due to packet loss or silent cloned node, transmissions from the source node will not be permitted. The verification messages of both a and a0 are broadcast in ring $O_a^\omega - 1, O_a^\omega \; and \; O_a^\omega + 1$ after that, both messages are received by the witness header Sa, and a revocation procedure is triggered. We describe the detail of the ERCD protocol in Algorithm. In addition to the normal operations, the recovery mechanism is very easy to be established based on ERCD protocol. For the case when the clone detection fails due to outage or clone attack, another clone detection cycle will be initiated and the source node will randomly choose a new route and forward the message enroot to a new witness header.

5. Performance Analysis

In this section, the performance of the ERCD protocol is evaluated in terms of clone detection probability, power consumption, and network lifetime. At first, we prove that the clone detection probability of the ERCD protocol under the scenario that witnesses are trustful in Section 5.1. After that, we derive the expression of energy consumption and network lifetime by using ERCD protocol.

5.1 Probability of clone detection:

In distributed clone detection protocol with random witnessselection, the clone detection probability generally refers towhether witnesses can successfully receive the verificationmessage from the source node or not. Thus, the clonedetection probability of ERCD protocol is the probabilitythat the verification message can be successfully transmittedfrom the source node to its witnesses. In ERCD protocol, theverification message is broadcast when it is near the witnessring, i.e., in the rings of $O_a^\omega - 1, O_a^\omega \& O_a^\omega$+1, to guarantee the network security. With such kind of method andassumption of trustful witnesses, we can prove that at leastone of the witnesses can receive the message, i.e., theclone attack can be detected with probability one. To simplifythe analysis, the transmission ranges of all sensornodes, r, are the same.

Algorithm: Energy and memory efficient clone detection protocol:

Phase 1

Step 1: Create a group of sensor nodes. The base station gives the different unique ID to each node and makes that node as original node.

Step 2: We divide a complete network into clusters.

Step 3: cluster head is selected in each cluster.

Phase 2

This phase-2 is applied for each separate cluster.

ERCD algorithm is applied for over all distributed network, so there is a delay in detecting the clone attack is more. In this paper we apply algorithm for different cluster group so the delay in detection of clone attack will get reduced. We can see that delay result. The concept of ERCD algorithm is used for fair comparison.

Step 4: A random value is distributed by using centralized mechanism like satellite or any other central stations.

Step 5: Each node board cast its ID and location to its claim.

Step 6: Neighbors receive the broadcast and each neighbors sends the claim.

Step 7: The claim is send to any of the location. This is selected using pseudo random function. (We are not using any ID to select the location).

Step 8: Before broadcasting, every node signs its message with its private key.

Step 9: Signature is verified at the destination end.

At the destination ends:

1. The signature check is carried out by verifying the received signature.

2. Message freshness: The ID and location information is extracted from received message. At the destination end it simply stores the ID and location if the claim node is first carrying that ID and location. If it receives the same ID and location for second time, it checks for the coherence for ID and location. This is the proof of detection of clone with two in-coherent claims.

Step 10: The incoherent ID and location is checked with cluster head and also with base station. It detects the clone node.

Step 11: clone node information is broadcasted to all other nodes. By this we can avoid the claim of the clone node with other nodes in the network.

Theorem 1:

Any two neighboring witnesses should be within the transmission ranges of each other. Considering that the width of each ring is r, we only need to ensure that the coverage of verification message on the witness ring arc is longer than r. Therefore, we focus on the proof that least r of circular arc in ring O_a^ω is covered by the three- ring broadcasts. We denote the broadcast nodes of the verification message in rings O_a^ω - 1, and O_a^ω + 1 by a1, a2 and a3, respectively. B1 and B2 are the borderlines between O_a^ω + 1, O_a^ω and O_a^ω - 1. LetΔ be the distance from the center point between B1 and B2 to node a2. We separate the proof into three cases, i) a2 locates at the center of ring O_a^ω, i.e., Δ=0, ii) a2 locates at the lower part of the ring O_a^ω and iii) a2 locates at the upper part of the ring O_a^ω. For the first case, the coverage of witness ring arc is longer than √3r, which is larger than r. For the second case, if d approaches 0 as shown in Fig. 3c, the coverage of witness ring arc is √3r which is larger than r. For the second case, if d approaches 0, the coverage of witness ring arc is √3r which is larger than r. Let Ca2 and Ca3 stand for the transmission ranges of node a2 and a3, respectively. b1, b2, b3 and b4 denote the intersections between B1, B2 and Ca2 , while b5 and b6 represent the intersections between Ca2 and Ca3 . It can be observed that the coverage of O_a^ω by the node on the circular arc like a3" is smaller than that of the node inside Ca2. Thus, we consider the worst case, i.e., a3 is on the circular arc of Ca2, to ensure the success of clone detection. To help proof the theorem, a coordinate system with a2 as the original point is constructed, where x-axis is parallel to B1 and B2,and y-axis is perpendicular to B1 and B2. We use i.x and i.y to represent the coordinate of node i. To ensure that the coverage is larger than r of witness ring arc, following inequality should be hold

Min (b_2.x,b_4.x,b_6.x) -max(b_1.x,b_3.x,b_5.x) > r; (1)

Where b_5.y < r/2 and b_6.y < r/2. Let β denote the angle between the line (a2, a3) and y-axis, then we can obtain.

$$\begin{cases} b_5 x = \dfrac{\frac{r\tan\beta}{2\cos\beta} - r\sqrt{\frac{\tan^2\beta}{4\cos^2\beta} - (1+\tan^2\beta)(\frac{1}{4\cos^2\beta} - 1)}}{1+\tan^2\beta} \\ b_6.x = \dfrac{\frac{r\tan\beta}{2\cos\beta} + r\sqrt{\frac{\tan^2\beta}{4\cos^2\beta} - (1+\tan^2\beta)(\frac{1}{4\cos^2\beta} - 1)}}{1+\tan^2\beta} \end{cases} \quad (2)$$

Let θ denote the angle between the line (a_2,b_4)and y-axis and θ =arc cos($\frac{\frac{r}{2}+\Delta}{r}$),βϵ (0, θ) We can get

$$\begin{cases} b_1.x = -\sqrt{\sqrt{0.75r^2 - \Delta^2} + \Delta r} \\ b_2.x = \sqrt{\sqrt{0.75r^2 - \Delta^2} + \Delta r} \\ b_3.x = -\sqrt{\sqrt{0.75r^2 - \Delta^2} - \Delta r} \\ b_4.x = \sqrt{\sqrt{0.75r^2 - \Delta^2} - \Delta r} \end{cases}$$

The coverage area is longer than r of witness ring arc. For the third case, it is obviously that the coverage area is longer than r of witness ring arc. Therefore, at least one of the witnesses can successfully receive the verification messages from node a and cloned nodes. At last, all the received messages will be forwarded to the witness header to determine whether the node is cloned or not.

5.2 Energy Consumption and Network Lifetime:

In WSNs, since wireless sensor nodes are usually poweredby batteries, it is critical to evaluate the energy consumptionof sensor nodes and to ensure that normal network operationswill not be broken down by node outage. Therefore, wedefine the network lifetime as the period from the start ofnetwork operation until any node outage occurs to evaluatethe performance of the ERCD protocol. We only consider thetransmission power consumption, as the reception powerconsumption occupies little percentage of total power consumption.Since witness sets in our ERCD protocol are generatedbased on ring structure, sensor nodes in the same ringhave similar tasks. To simplify the analysis, we suppose thatall sensor nodes in the same ring have same traffic load. Ouranalysis in this work is generic, which can be applied to variousenergy models. Let $\varepsilon 1$ and $\lambda 1$ denote the bit size of eachcollected data and the frequency of data collection, respectively.

A node inside ring k refers to the node whichlocates in the ring with index smaller than k.First, we analyze the traffic load of each sensor node,such that the energy consumption and network lifetime canbe derived based on it. By using the ERCD protocol, trafficload of each sensor node consists of normal data collection,witness selection and legitimacy verification. We can derivethe expression for the traffic load of normal data collectionas follows.

Theorem: 2.The traffic load of each sensor node for legitimacy verification in ring k, denoted d_k^v, is

$$\boldsymbol{d_k^v} = \begin{cases} \dfrac{\boldsymbol{k^2\varepsilon_2\lambda_2}}{\boldsymbol{2k-1}}, \boldsymbol{k \le \emptyset} \\ \dfrac{[(\boldsymbol{h-k})(\boldsymbol{k-1})^2+(\boldsymbol{h^2-k^2})(\boldsymbol{k-\emptyset})+\boldsymbol{\pi k h^2}]\boldsymbol{\varepsilon_2\lambda_2}}{(\boldsymbol{h-\emptyset})(\boldsymbol{2k-1})} + \boldsymbol{\varepsilon_2\lambda_2}, \boldsymbol{k > \phi}. \end{cases}$$

- Eq. (i)

Proof: We calculate the traffic load for legitimacy verification of each node according to the position of the node i.e., whether the node is located outside ∅ or not. If the node does not locate outside ring ∅, the traffic for legitimacy verification is transmitted from nodes inside ring k to nodes outside ring k, which is $\pi(kr)^2 \rho\varepsilon_2\lambda_2$. As the number of sensor nodes in ring k

is $N_k = \pi(2k-1)r^2\rho$,the traffic load for legitimacy verification of each node in ring k; k <∅ , can be expressed as

$$d_k^v = \frac{k^2\varepsilon_2\lambda_2}{2k-1}, k \le \emptyset \quad \text{- Eq. (ii)}$$

If the node locates outside ring ∅, the verification traffic load is composed of the traffic transmitted to the witness ring and the traffic forwarded to the witness header,$d_k^v = d_k^{v1} + d_k^{v2}$ The traffic transmitted to the witness ring can be further divided into three different cases: 1) traffic sent from nodes inside ring k to nodes outside ring k,2) traffic sent by nodes in ring k, and 3) traffic sent from nodes outside ring k to nodes inside ring k. For the first case,(h-k)/(h-∅) of the traffic is sent to the nodes outside of ring k, and the traffic sent by the nodes inside ring k is $\pi((k-1)r)^2\ \rho\varepsilon_2\lambda_2$. Therefore the traffic relayed by nodes in ring k for the first case is $\pi((k-1)r)^2\ \rho\varepsilon_2\lambda_2$(h-k)/(h-∅) . For the second case, the traffic sent by nodes in ring k is $\pi(2k-1)r^2\ \rho\varepsilon_2\lambda_2$. For the third case, the traffic can be calculated by the similar method in the first case, which is $\pi r^2(h^2-k^2)\rho\varepsilon_2\lambda_2$(k-∅)/(h-∅) . Thus, the verification traffic load by each node in ring k >∅ to the witness ring can be expressed as

$$d_k^{v1} = \frac{\left[\frac{(h-k)(k-1)^2}{h-\emptyset} + \frac{(h^2-k^2)(k-\emptyset)}{h-\emptyset}\right]\varepsilon_2\lambda_2}{2k-1} + \varepsilon_2\lambda_2, k > \phi \text{- Eq. (iii)}$$

After that, we try to obtain the traffic load for forwarding verification to the witness header in the witness ring. We first calculate the verification traffic load of witness ring k, which is $\pi(hr)^2\rho\varepsilon_2\lambda_2/(h-\phi)$. As the verification is only forwarded along at most half of the circumference to reach the witness header, the hop length of the forwarding will not exceed πk. Based on the number of sensor nodes in ring k, $\pi(2k-1)r^2\ \rho$, the traffic load for forwarding verification to the witness header can be expressed $d_k^{v2} = \frac{\pi k h^2\varepsilon_2\lambda_2}{[(h-\phi)(2k-1)]}, k > \phi.$ Overall, the traffic load of each sensor node for legitimacy verification can be expressed in Eq. (i). At last, we derive the expression of the traffic load for witness selection by using ERCD protocol. Let stand for the frequency of witness selection.

Theorem 3: The traffic load for witness selection of each node in rig k, denoted byd_k^w , can be expressed as :

$$d_k^w = \begin{cases} \frac{d_k^{v1}\lambda_3}{\lambda_2}, k \le \emptyset \\ \frac{d_k^{v1}\lambda_3}{\lambda_2} + \frac{2\pi k h^2\varepsilon_2\lambda_3}{(h-\phi)(2k-1)}, k > \emptyset. \end{cases} \text{-Eq. (iv)}$$

Proof: By using ERCD protocol, the traffic load of clone detection consists of witness selection and legitimacy verification. In witness selection, there are two steps: 1) the private information of the source node is sent to its witness ring; and 2) the private information is forwarded along the witness ring to construct a ring structure; in legitimacy verification, there are also two steps: 1) the verification message is first sent to the witness ring of the source node, and 2) the message is forwarded to the witness header. We can observe that, for each witness selection and legitimacy verification, the traffic load by each sensor of first step is the same, i.e. d_k^{v1}.

When we know $\lambda_1, \lambda_2, \lambda_3, \varepsilon_1$and ε_2 , we can derive the optimal ∅ to maximize the network lifetime with $d_k^t = d_k^c + d_k^v + d_k^w$

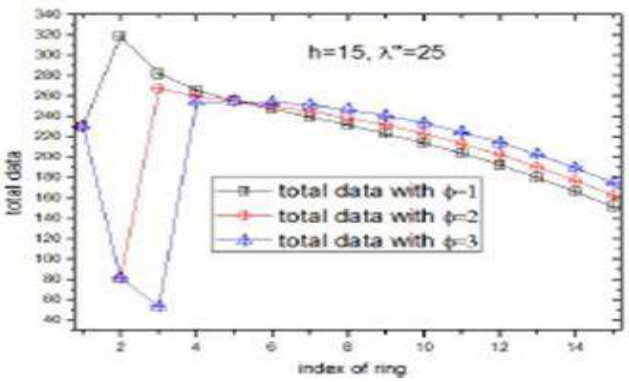


Figure 3: Traffic load distribution with various

As shown in Figure 3, ∅ has significant impact on the energy consumption of sensor nodes. When is ∅ 1; 2 and 3, sensor nodes with ring indices 2; 3, and 5 consume the maximal energy throughout the WSN, respectively. Thus, the network lifetime can be determined by different values of ∅ , and it is critical to obtain the optimal ∅ to maximize the network lifetime. Let g, p and α denote the number of witnesses selected by each neighbor, the probability that a neighbor will copy position information, and the average node degree in the network, respectively. To evaluate the performance, we compare the ERCD protocol with some existing protocols in terms of network lifetime.

6. Experiment Results:

To evaluate the performance of ERCD protocol, the NS2 a well-known open source modular simulation platform for large network, is used in our simulations. As the NS2 is a discrete event-driven system, the future event set is stored in the system, and events are released one by one to evaluate our ERCD protocol in the simulation. The transmission range of each sensor node is r = 40 m. In the simulation, data and verification request messages are of the same size for simplicity, i.e., ε1 = ε 2 =100 bytes. Each cycle of witness selection is followed by a data collection cycle, λ1 = λ 3=1, and the frequency of legitimacy verification is set as λ 2 = 10. We set the amount of non-witness rings ϖ as 1. The frequency of clone detection can be determined according to the practical requirement, e.g., once a day for temperature measurement in forest.

In Figure 4, we present the case that witnesses will be compromised, and therefore clone detection could fail because of modification of verification messages by compromised witnesses. For untrustful witnesses, since any witness has permission to scan the data of verification messages from the source node, compromised witnesses will scan the verification

 ISSN: 2321-8169
471 – 478

message, and modify the verification message before forwarding it to alternative witnesses. Witness nodes is also compromised however it's arduous to find it. Since BSs cannot find out whether or not the received verification message is that the original copy or not, it's going to be tough to effectively decide that witness is compromised.

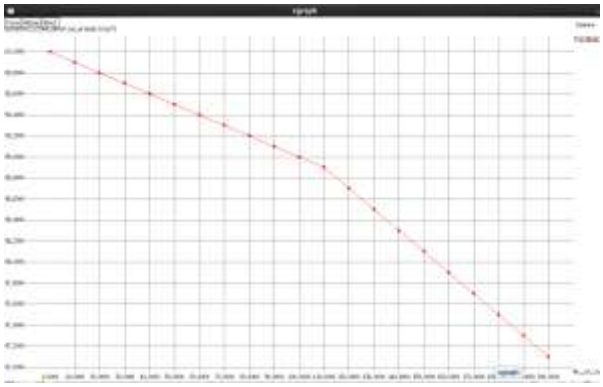
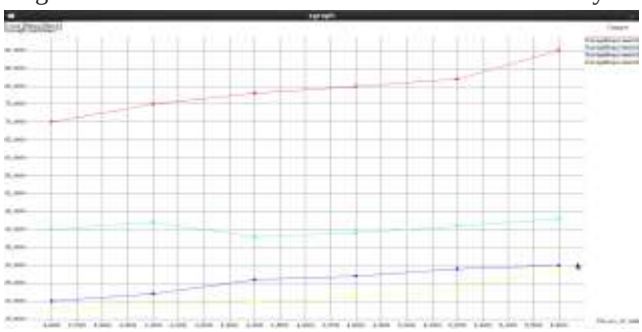
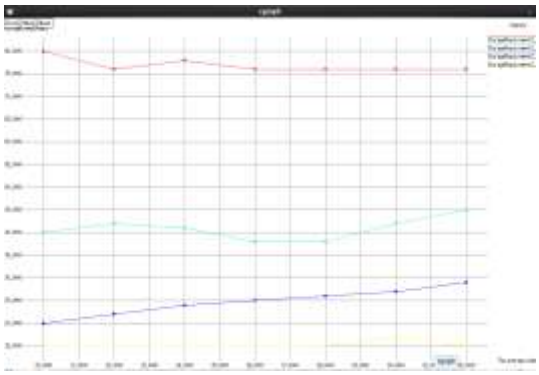


Figure 4: Clone Detection Probability

We compare the specified information buffer with varied node densities by using ERCD or some existing protocols in Figure 5. ERCD protocol considerably outperforms the LSM, however needs a lot of information buffer than RED and P-MPC, under the situations of various node densities. Examination with the LSM protocol, the storage necessities of ERCD, RED and P-MPC protocols don't increase with the expansion of node number. This is often as a result of the witness range of LSM depends on the node number whereas alternative protocols doesn't, which might accomplish lower storage demand with a lot of node number or node density.

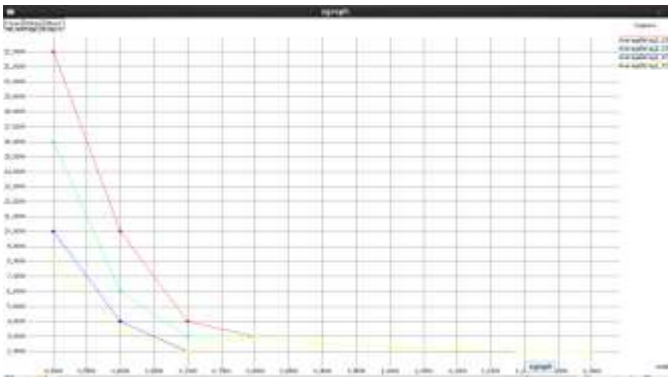


a) **Different node numbers**



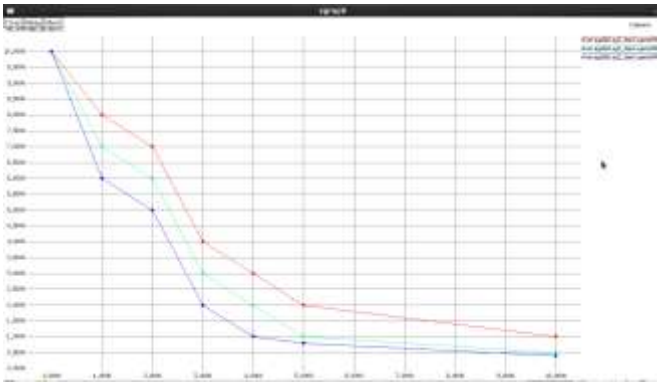
b) **Different average node**

Figure 5: Required data buffer using ERCD protocol



a) **Different number of node**

The relationship of average delay, duty cycle and node density is shown in Fig. 16. The average delay is very small when node density is larger than 1.8 nodes/m2, and the average delay of sensor nodes decreases significantly with the increase of duty cycles from 0 to 0.05.



b) **Different duty**

Figure 6 Average delay by using ERCD

CONCLUSION

Thus after identifying the weaknesses of proposed methods which has been done previously we proposed an efficient algorithm that covers various issues related to it. Using proposed algorithm it is possible to minimize the overhead of data packets. We have proposed distributed energy-efficient clone detection protocol with random witness selection. Specifically, we have proposed ERCD protocol, which includes the witness selection and legitimacy verification stages. Both of our theoretical analysis and simulation results have demonstrated that our protocol can detect the

Clone attack with almost probability 1, since the witnesses of each sensor node is distributed in a ring structure which makes it easy be achieved by verification message. In addition, our can achieve better network lifetime and total energy protocol consumption with reasonable storage capacity of data buffer. This is because we take advantage of the location information by distributing the traffic load all over

WSNs, such that the energy consumption and memory storage of the sensor nodes around the sink node can be relieved and the network lifetime can be extended.

In our future work, we will consider different mobility patterns under various network scenarios and improve the connectivity in sparse network number of mobile sink could be increased. Simulations can be extended with multiple mobile sink to cover the other parameters and scenarios such as fault tolerance, throughput and impact of data aggregation etc. Link failure due to the mobility of sink and node failure could also be taken into consideration for maintaining the reliable path.

ACKNOWLEDGMENT

The authors would really like to CSE Department and Principal of TGPCET TulsiramGaiyakwadPatil college of Engineering & Technology providing their support and facilities like labs, software's etc. needed to carry out this work.

REFERENCES

[1] Z. Zheng, A. Liu, L. X. Cai, Z. Chen, and X. Shen, "ERCD: An energy-efficient clone detection protocol in WSNs," in Proc. IEEE INFOCOM, Apr. 14-19, 2013, pp. 2436–2444.

[2] R. Lu, X. Li, X. Liang, X. Shen, and X. Lin, "GRS: The green, reliability, and security of emergingmachine to machine communications," IEEE Commun.Mag., vol. 49, no. 4, pp. 28–35, Apr. 2011.

[3] A. Liu, J. Ren, X. Li, Z. Chen, and X. Shen, "Design principles and improvement of cost function based energy aware routing algorithms for wireless sensor networks," Comput. Netw., vol. 56, no. 7, pp. 1951–1967, May. 2012.

[4] T. Shu, M. Krunz, and S. Liu, "Secure data collection in wireless sensor networks using randomized dispersive routes," IEEE Trans. Mobile Comput., vol. 9, no. 7, pp. 941–954, Jul. 2010.

[5] P. Papadimitratos, J. Luo, and J. P. Hubaux, "A randomized countermeasure against parasitic adversaries in wireless sensor networks," IEEE J. Sel. Areas Commun., vol. 28, no. 7,pp. 1036–1045, Sep. 2010.

[6] R. Lu, X. Lin, T. H. Luan, X. Liang, and X. Shen, "Pseudonym changing at social spots: An effective strategy for location privacy in VANETs," IEEE Trans. Veh. Technol., vol. 61, no. 1, pp. 86–96, Jan. 2012.

[7] Z. M. Fadlullah, M. Fouda, N. Kato, X. Shen, and Y. Nozaki, "An early warning system against malicious activities for smart grid communications," IEEE Netw., vol. 25, no. 5, pp. 50–55, May. 2011.

[8] R. Lu, X. Lin, X. Liang, and X. Shen, "A dynamic privacy-preserving key management scheme for location based services in VANETs," IEEE Trans. Intell. Transp. Syst., vol. 13, no. 1, pp. 127–139, Jan. 2012.

[9] M. Conti, R. D. Pietro, L. Mancini, and A. Mei, "Distributed detection of clone attacks in wireless sensor networks," IEEE Trans.Dependable. Secure Comput., vol. 8, no. 5, pp. 685–698, Sep.-Oct. 2011.

[10] M. Conti, R. D. Pietro, L. Mancini, and A. Mei, "Distributed detection of clone attacks in wireless sensor networks," IEEE Trans.Dependable. Secure Comput., vol. 8, no. 5, pp. 685–698, Sep.-Oct. 2011.

[11] Y. Zeng, J. Cao, S. Zhang, S. Guo, and L. Xie, "Random-walk based approach to detect clone attacks in wireless sensor networks,"IEEE J. Sel. Areas Commun., vol. 28, no. 28, pp. 677–691, Jun. 2010.

[12] B. Zhu, S. Setia, S. Jajodia, S. Roy, and L. Wang, "Localized multicast: Efficient and distributed replica detection in large-scale sensor networks," IEEE Trans. Mobile Comput., vol. 9, no. 7, pp. 913–926, Jul. 2010.

[13] H. Chan, A. Perrig, and D. Song. Random key predistribution schemes for sensor networks. In *Proceedings* of 2003 IEEE Symposium on Security and Privacy (S&P *'03)*, pages 197–213, 2003.

[14] J. R. Douceur. The sybil attack. In *Proceedings of the 1st*International Workshop on Peer-to-Peer Systems (IPTPS *'01)*, pages 251–260. Springer, 2002.

[15] L. Eschenauer and V. D. Gligor. A key-management scheme for distributed sensor networks. In *Proceedings of the 9th*ACM Conference on Computer and Communications *Security (CCS '02)*, pages 41–47, 2002.

[16] J. Newsome, E. Shi, D. Song, and A. Perrig. The sybil attack in sensor networks: analysis & defenses. In *Proceedings of ACM IPSN'04*, pages 259–268, 2004.

[17] Y. Xuan, Y. Shen, N. P. Nguyen, and M. T. Thai, "A trigger identification service for defending reactive jammers in WSN," IEEE Trans. Mobile Comput., vol. 11, no. 5, pp. 793–806, May. 2012.

[18] R. Lu, X. Lin, H. Zhu, X. Liang, and X. Shen., "BECAN: A bandwidth-efficient cooperative authentication scheme for filtering injected false data in wireless sensor networks," IEEE Trans. Parallel Distrib. Syst., vol. 23, no. 1, pp. 32–43, Jan. 2012.

[19] B. Parno, A. Perrig, and V. D. Gligor. Distributed detection of node replication attacks in sensor networks. In Proceedings of 2005 IEEE Symposium on Security and *Privacy (S&P '05)*, pages 49–63, 2005.

[20] C.-S. Ok, S. Lee, P. Mitra, S. Kumara, Distributed energy balanced routing for wireless sensor networks, Comput. Ind. Eng. 57 (1) (2009) 125–135.

[21] W.R. Heinzelman, A. Ch, H. Balakrishnan, Energy-efficient communication protocol for wireless microsensor networks, in: Proceedings of the 33rd Hawaii International Conference on System Sciences,2000.

[22] C-S. Ok, S. Lee, P. Mitra, S. Kumara, Distributed routing in wireless sensor networks using energy welfare metric, Inform. Sci. 180 (2010) 1656–1670.

[23] IEEE.802.11, Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specification, IEEE std. 802.11-1999 ed., 1999.

[24] Q. Wang, W. Yang, Energy consumption model for power management in wireless sensor networks, in: 4th Annual IEEE Communications Society Conference on Sensor, Mesh and Ad Hoc Communications and Network (SECON'2007), 2007, pp. 142–151.

[25] M. Stemm, R.H. Katz, Measuring and reducing energy consumption of network interface in hand-held devices, IEICE Trans. Commun. E80-B (8) (1997) 1125–1131.