**Energy and Memory Efficient Clone Detection in Wireless Sensor Networks**

**ABSTRACT:**

In this paper, we propose an energy-efficient location-aware clone detection protocol in densely deployed WSNs, which can guarantee successful clone attack detection and maintain satisfactory network lifetime. Specifically, we exploit the location information of sensors and randomly select witnesses located in a ring area to verify the legitimacy of sensors and to report detected clone attacks. The ring structure facilitates energy-efficient data forwarding along the path towards the witnesses and the sink. We theoretically prove that the proposed protocol can achieve 100 percent clone detection probability with trustful witnesses. We further extend the work by studying the clone detection performance with untrustful witnesses and show that the clone detection probability still approaches 98 percent when 10 percent of witnesses are compromised. Moreover, in most existing clone detection protocols with random witness selection scheme, the required buffer storage of sensors is usually dependent on the node density, i.e., Oð ffiffiffinpÞ, while in our proposed protocol, the required buffer storage of sensors is independent of n but a function of the hop length of the network radius h, i.e., OðhÞ. Extensive simulations demonstrate that our proposed protocol can achieve long network lifetime by effectively distributing the traffic load across the network.

**EXISTING SYSTEM:**

* To allow efficient clone detection, usually, a set of nodes are selected, which are called witnesses, to help certify the legitimacy of the nodes in the network. The private information of the source node, i.e., identity and the location information, is shared with witnesses at the stage of witness selection. When any of the nodes in the network wants to transmit data, it first sends the request to the witnesses for legitimacy verification, and witnesses will report a detected attack if the node fails the certification. To achieve successful clone detection, witness selection and legitimacy verification should fulfill two requirements: 1) witnesses should be randomly selected; and 2) at least one of the witnesses can successfully receive all the verification message(s) for clone detection.
* Randomized Efficient and Distributed protocol (RED) and Line-Select Multicast protocol (LSM) use up their batteries due to the unbalanced energy consumption, and dead sensors may cause network partition, which may further affect the normal operation of WSNs.

**DISADVANTAGES OF EXISTING SYSTEM:**

* Is to make it difficult for malicious users eavesdrop the communication between current source node and its witnesses, so that malicious users cannot generate duplicate verification messages.
* The existing system does not make sure that at least one of the witnesses can check the identity of the sensor nodes to determine whether there is a clone attack or not.
* Does not guarantee a high clone detection probability, i.e., the probability that clone attacks can be successfully detected, it is critical and challenging to fulfill these requirements in clone detection protocol design.
* The design criteria of clone detection protocols for sensor networks should not only guarantee the high performance of clone detection probability but also consider the energy and memory efficiency of sensors.
* The first occurrence of a sensor that runs out of energy, it is critical to not only minimize the energy consumption of each node but also balance the energy consumption among sensors distributively located in different areas of WSNs

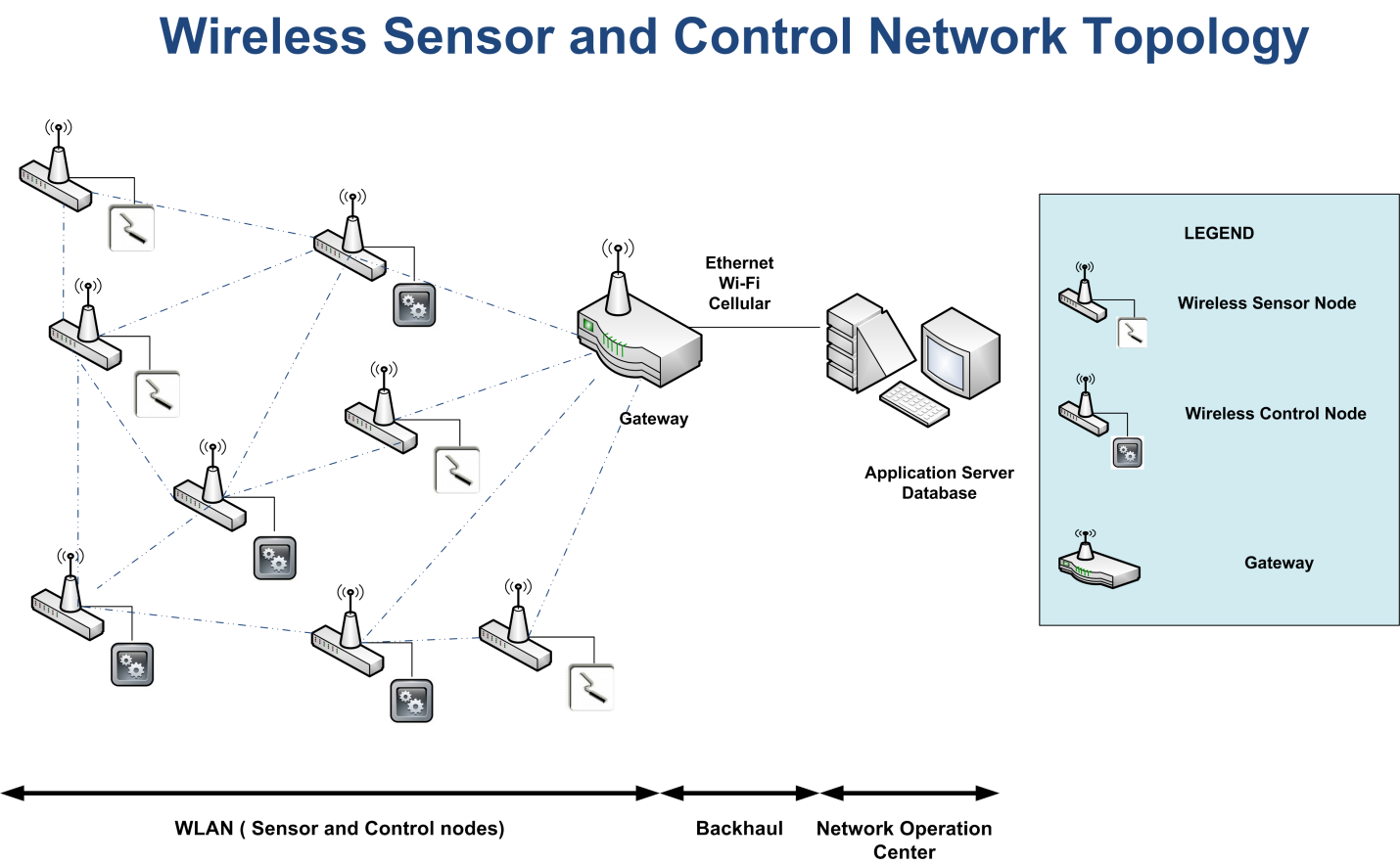
**PROPOSED SYSTEM:**

* In this paper, besides the clone detection probability, we also consider energy consumption and memory storage in the design of clone detection protocol, i.e., an energy- and memory-efficient distributed clone detection protocol with random witness selection scheme in WSNs.
* Our protocol is applicable to general densely deployed multi-hop WSNs, where adversaries may compromise and clone sensor nodes to launch attacks.
* We extend the analytical model by evaluating the required data buffer of ERCD protocol and by including experimental results to support our theoretical analysis. Energy-Efficient Ring Based Clone Detection (ERCD) protocol.
* We find that the ERCD protocol can balance the energy consumption of sensors at different locations by distributing the witnesses all over WSNs except non-witness rings, i.e., the adjacent rings around the sink, which should not have witnesses.
* After that, we obtain the optimal number of non-witness rings based on the function of energy consumption.
* Finally, we derive the expression of the required data buffer by using ERCD protocol, and show that our proposed protocol is scalable because the required buffer storage is dependent on the ring size only.

**ADVANTAGES OF PROPOSED SYSTEM:**

* The performance of the ERCD protocol is evaluated in terms of clone detection probability, power consumption, network lifetime, and data buffer capacity.
* Extensive simulation results demonstrate that our proposed ERCD protocol can achieve superior performance in terms of the clone detection probability and network lifetime with reasonable data buffer capacity.
* The experiment results demonstrate that the clone detection probability can closely approach 100 percent with untrustful witnesses.
* By using ERCD protocol, energy consumption of sensors close to the sink has lower traffic of witness selection and legitimacy verification, which helps to balance the uneven energy consumption of data collection.

**SYSTEM ARCHITECTURE:**



**BLOCK DIAGRAM:**

****

**MODULES:**

* System Construction Module
* ERCD Protocol
* Probability of Clone Detection
* Energy Consumption and Network Lifetime
* **MODULES DESCSRIPTION:**

**System Construction Module**

* In the first module, we develop the System Construction Module, to evaluate and implement our proposed system. In this module, we consider a network region with one base station (BS) and an enormous number of wireless sensor nodes randomly distributed in the network.
* We use the sink node as the origin of the system coordinator. Based on the location of the BS, the network region is virtually separated into adjacent rings, where the width of each ring is the same as the transmission range of sensor nodes. The network is a densely deployed WSN, i.e., i) for each node, there exist sensor nodes located in each neighboring ring, and ii) for each ring, in each ring, there are enough sensor nodes to construct a routing path along the ring.
* The network model can be simply extended into the case of multiple BSs, where different BSs use orthogonal frequency-division multiple access (OFDMA) to communication with its sensor nodes. For each sensor, it has to accomplish the tasks of data collection as well as clone detection. In every data collecting cycle, sensors send the collected data to the sink node through multi-hop paths.
* Buffer storage capacity should be sufficient to store the private information of source nodes, such that any node can be selected as a witness. When the buffer storage of the sensor node is full, the oldest information will be dropped to accept the latest incoming information.

**ERCD Protocol**

* In this module, we introduce our distributed clone detection protocol, namely ERCD protocol, which can achieve a high clone detection probability with little negative impact on network lifetime and limited requirement of buffer storage capacity.
* The ERCD protocol consists of two stages: witness selection and legitimacy verification. In witness selection, a random mapping function is employed to help each source node randomly select its witnesses. In the legitimacy verification, a verification request is sent from the source node to its witnesses, which contains the private information of the source node. If witnesses receive the verification messages, all the messages will be forwarded to the witness header for legitimacy verification, where witness headers are nodes responsible for determining whether the source node is legitimacy or not by comparing the messages collected from all witnesses. If the received messages are different from existing record or the messages are expired, the witness header will report a clone attack to the sink to trigger a revocation procedure.

**Probability of Clone Detection**

* In this module, we focus on designing a distributed clone detection protocol with random witness selection by jointly considering clone detection probability, network lifetime and data buffer storage. Initially, a small set of nodes are compromised by the malicious users. Utilizing the clone detection protocol, we aim at maximizing the clone detection probability, i.e., the probability that cloned node can be successfully detected, to ensure the security of WSNs; meanwhile, the sufficient energy and buffer storage capacity for data collection and operating clone detection protocol should be guaranteed, which means that the network lifetime, i.e., the period from the start of network operation until the first outage occurs, should not be impacted by the proposed clone detection protocol with sensors’ buffer storage.
* In distributed clone detection protocol with random witness selection, the clone detection probability generally refers to whether witnesses can successfully receive the verification message from the source node or not. Thus, the clone detection probability of ERCD protocol is the probability that the verification message can be successfully transmitted from the source node to its witnesses.
* In ERCD protocol, the verification message is broadcast when it is near the witness ring, to guarantee the network security.

**Energy Consumption and Network Lifetime**

* In WSNs, since wireless sensor nodes are usually powered by batteries, it is critical to evaluate the energy consumption of sensor nodes and to ensure that normal network operations will not be broken down by node outage. Therefore, we define the network lifetime as the period from the start of network operation until any node outage occurs to evaluate the performance of the ERCD protocol.
* We only consider the transmission power consumption, as the reception power consumption occupies little percentage of total power consumption. Since witness sets in our ERCD protocol are generated based on ring structure, sensor nodes in the same ring have similar tasks. To simplify the analysis, we suppose that all sensor nodes in the same ring have same traffic load.
* Our analysis in this work is generic, which can be applied to various energy models. A node inside (outside) ring k refers to the node which locates in the ring with index smaller than (larger than) k. First, we analyze the traffic load of each sensor node, such that the energy consumption and network lifetime can be derived based on it. By using the ERCD protocol, traffic load of each sensor node consists of normal data collection, witness selection and legitimacy verification.

**SYSTEM REQUIREMENTS:**

**HARDWARE REQUIREMENTS:**

* System : Pentium Dual Core.
* Hard Disk : 120 GB.
* Monitor : 15’’ LED
* Input Devices : Keyboard, Mouse
* Ram : 1GB.

**SOFTWARE REQUIREMENTS:**

* Operating system : Windows 7.
* Coding Language : JAVA/J2EE
* Tool : Netbeans 7.2.1
* Database : MYSQL

**REFERENCE:**

Zhongming Zheng, Student Member, IEEE, Anfeng Liu, Member, IEEE, Lin X. Cai, Member, IEEE, Zhigang Chen, Member, IEEE, and Xuemin (Sherman) Shen, Fellow, IEEE, “Energy and Memory Efficient Clone Detection in Wireless Sensor Networks”, **IEEE TRANSACTIONS ON MOBILE COMPUTING, VOL. 15, NO. 5, MAY 2016.**