ISSN (Online) 2321 – 2004
ISSN (Print) 2321 – 5526

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH IN ELECTRICAL, ELECTRONICS, INSTRUMENTATION AND CONTROL ENGINEERING
Vol. 2, Issue 12, December 2014

A Review -Detection & alleviation of Clone Attacks in Wireless Sensor Networks

Manjunatha R C [1], Dr. Rekha K R [2], Dr. Nataraj K R [3]

Research scholar, Jain University Bangalore, India[1]

Professor, department of ECE, SJBIT Bangalore, India[2]

Professor and Head, Department of ECE, SJBIT Bangalore, India[3]

Abstract: Wireless Sensor Networks (WSNs) offer an excellent opportunity to monitor environments, and have a lot of interesting applications, some of which are quite sensitive in nature and require full proof secured environment. The security mechanisms used for wired networks cannot be directly used in sensor networks as there is no user-controlling of each individual node, wireless environment, and more importantly, scarce energy resources. In this research, we consider a typical threat known as clone node attack, where an adversary creates its own low-cost sensor nodes called clone nodes and misinforms the network to acknowledge them as legitimate nodes. To instigate this attack, an adversary only needs to physically capture one node, and after collecting all secret credentials, an adversary clones the sensor node and deploys one or more clones of the compromised node into the network at strategic positions, damaging the whole network by carrying out many internal attacks. Detecting the node clone attack has become an imperative research topic in sensor network security, and designing detection schemes against node clone attack involves different threatening issues and challenges. In this review, we have classified the existing detection schemes and comprehensively explore various suggestions in each category as to demonstrate limitations of the existent detections as well as effective contributions.

Keywords: Clone Attack, Wireless Sensor Network, Network Security, WSN, Review.

I INTRODUCTION

Advancement in technology has made it possible to develop tiny low-cost sensor nodes with off-the-shelf hardware. A wireless sensor network (WSN), which is a distributed and self-organized network, is a collection of such sensor nodes with limited resources that collaborate in order to achieve a common goal. These sensor nodes are comprised of low-cost hardware components with constraints on battery life, memory size, and computation capabilities [1]. Wireless sensor networks are often deployed in harsh and hostile environments which are inaccessible and even hazardous areas to perform various monitoring tasks. For example, they can be used to monitor factory instrumentation, pollution levels, freeway traffic, and the structural integrity of buildings [2]. Some of the other applications of WSNs include patient monitoring, climate sensing, control in office buildings, and home environmental sensing systems for temperature light, moisture, and motion.

WSNs are viable solutions for a wide variety of real-world challenges; however, a set of new security challenges arise in sensor networks due to the fact that current sensor nodes lack hardware support for tamper-resistance (because it is uneconomical to enclose each node in a tamper resistant hardware) and are often deployed in unattended environments where they are vulnerable to capture and compromise by an adversary. Taking an example of a battlefield, WSNs must tackle the threats and attacks from attackers because these areas are sometimes physically accessible to camouflaged enemies [3] who would like to acquire the private locations of soldiers from or inject wrong commands into the sensor network [4]. Similarly, an unattended WSN can be deployed in hostile environments which imply the existence of an adversary. For example, WSN can be used to monitor firearm discharge, illicit crop cultivation, drug/weapons smuggling, human trafficking, nuclear emissions in a rogue region and other illegal activities [5]. Thus, it is very important to ensure the security of sensor networks in such scenarios.

The unattended nature of wireless sensor networks can be exploited by adversaries which are able to launch an array of different physical attacks including node clone attack, signal or radio jamming, denial of service (DoS) attack, node outage, eavesdropping, and Sybil attack and other attacks like sinkhole, wormhole, and selective forwarding attack. Threats to sensor networks can be either layer dependent or layer independent. Attacks in the former category can be application dependant and are specific to different OSI layers targeting specific network functionalities such as routing, node localization, time synchronization, and data aggregation, while the attacks in the latter category are application independent affecting a wide variety of applications from object tracking and fire alarming to battlefield surveillance, and these attacks are not launched on any OSI layer. The attacks of the latter category are also application independent [2]. This attack taxonomy is also shown in Figure 1. In order to protect wireless sensor networks from layer dependent attacks, many schemes have been proposed. To alleviate the effects of routing disruption attacks, secure routing schemes have been proposed [6, 7]. Authentication schemes [8–10] are used to mitigate false data injection attacks. Data aggregation can be secured by using secure data aggregation protocols proposed in [11–14]. To defend

ISSN (Online) 2321 – 2004
ISSN (Print) 2321 – 5526

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH IN ELECTRICAL, ELECTRONICS, INSTRUMENTATION AND CONTROL ENGINEERING
Vol. 2, Issue 12, December 2014

localization and time synchronization protocols from different attacks, and threats many protocols have been proposed in [15–21]. Nevertheless, most of these schemes are attack resilient, rather than they can detect and remove the source of attack. Thus, there is a need to detect and revoke the sources of attacks as soon as possible to substantially reduce the costs and damages incurred by employing attack resilient approaches.

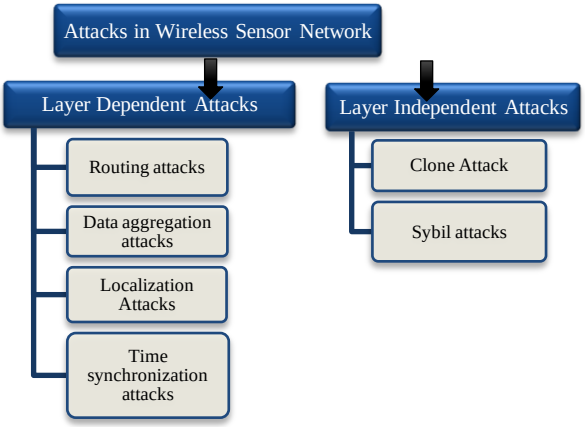

Figure 1: Classification of attacks on wireless sensor networks.

In this review, we consider a very severe and important physical attack on WSN which is called clone attack. It is also known as identity attack. In this attack, an adversary first physically captures only one or few of legitimate nodes, then clones or clones them fabricating those clones having the same identity (ID) with the captured node, and finally deploys a capricious number of clones throughout the network. This whole process of node clone attack and the various stages are shown in Figure 2. This vexing problem arises from the actuality that sensor nodes are unshielded. It is stated in [22] that an experienced attacker can completely compromise a typical sensor node by using only a few readily available tools, and it can then obtain copies of that node memory and data within 1 min of discovering it. The clones or clones may even be selectively reprogrammed to subvert the network by launching further insider attacks like falsifying sensor data or suppressing legitimate data, extracting data from the network and disconnect the network by triggering correct execution of node revocation protocols that rely on threshold voting schemes and staging denial of service (DoS) attacks. Clone nodes may create a black hole, initiate a wormhole attack with a collaborating adversary, or may also leak data in an environment in which sensed data must be kept private [23]. If these cloned nodes or clones remain undetected or unattended for a long time, they can further commence the changes in protocol behavior and intrusion into the systems security [24]. It is easy for an adversary to launch such attacks due to the fact that the clones, created by an adversary, have legitimate information (codes, key materials, and credentials), and they may be considered as legitimate nodes and totally honest by its neighbors which are participating in the network operation in the same way as the non-compromised nodes.

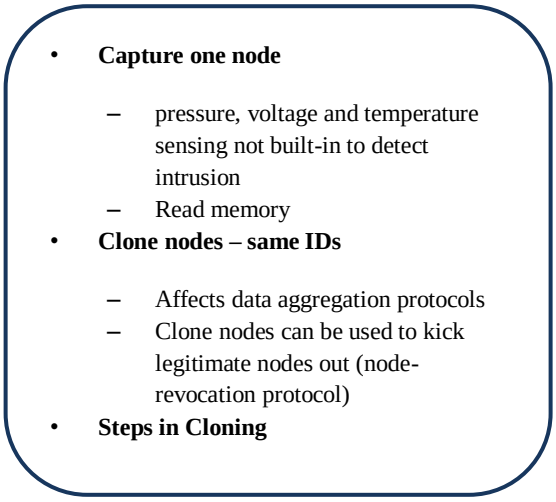

Figure 2: Steps of node clone attack.

The above mentioned traditional security schemes for WSNs are inept to detect and prevent node clone attack. Thus, in the last few years, a number of detection and prevention techniques/schemes have been proposed in the literature. According to [2], the detection schemes are classified on a high level as network-based or radio-based detection. Only one instance of radio-based detection is found in [25].

A WSN can be either stationary or mobile. In static wireless sensor networks (SWSNs), the sensor nodes are stationary or static; that is, the sensor nodes are deployed randomly, and after deployment their positions do not change. On the other hand, in mobile wireless sensor networks (MWSNs), the sensor nodes can move on their own, and after deployment, they can interact with the physical environment by controlling their own movement. Advances in robotics have made it possible to develop such mobile sensors which are autonomous and have the ability to sense, compute, and communicate like static sensors. The prime difference between static and mobile WSNs is that mobile nodes are able to reposition and organize themselves in the network, and after initial deployment, the nodes spread out to gather information [26, 27]. Mobile nodes can communicate with one another when they are within the range of each other, and only then they can exchange their information gathered by them. Another important difference is that in static WSNs fixed routing or flooding is used for data distribution, while in mobile WSNs dynamic routing is used. As static and mobile WSNs differ in their characteristics hence clone detection schemes for stationary and mobile WSNs will be substantially different. In a static or stationary WSN, a sensor node has a unique deployment position, and thus if one logical node ID is found to be associated with two or more physical locations, node clone is detected. But this is inapplicable to mobile WSNs where sensor nodes keep roaming in the deployment field. So, clone detection in such mobile WSN involves different scenarios and techniques.

For mobile WSNs, both centralized and distributed techniques have been proposed in the literature. In the case of stationary WSNs, centralized techniques are further

ISSN (Online) 2321 – 2004
ISSN (Print) 2321 – 5526

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH IN ELECTRICAL, ELECTRONICS, INSTRUMENTATION AND CONTROL ENGINEERING
Vol. 2, Issue 12, December 2014

categorized into five types, namely, straightforward base station-based technique, key usage-based technique, SET operations techniques, cluster head-based techniques and neighbourhood social signature-based techniques. The distributed techniques for stationary WSNs are further divided into four types naming Node to Network Broadcasting, claimer-reporter-witness-based techniques, neighbour-based and generation- or group-based techniques. On the other hand, mobile centralized detection techniques are further divided into two types including key usage-based and node speed-based techniques. The mobile distributed detection techniques are divided into three main types, namely, node meeting-based, mobility-assisted-based, and information-exchange-based techniques.

Some of the Clone detection on Network-based schemes can be summarized as

- *Straightforward base station based techniques*
- *Key usage-based techniques*
- *SET operations-based techniques*
- *Cluster head-based techniques*
- *Neighbourhood social signature based techniques*
- *Node to network broadcasting based techniques*
- *Node Speed based techniques*
- *Node meeting based techniques*
- *Mobility assisted based techniques*
- *Information exchange based techniques*
- *Generation or group based techniques*

Clone Attacks in Wireless Sensor Network

With the rapid use of vast technologies in WSNs, the threats and attacks to WSN are escalating and are also being diversified and deliberate. A typical threat called node clone attack is a very severe and niggling problem in which an adversary clones a sensor node after physically capturing it and then uses these clones to disrupt the network operations by redeploying them at strategic positions of the network. Thus the research related to node clone attack in WSNs has been followed with much interest in recent years. The research of authentication and security techniques is already quite mature but such solutions fail to detect node clone attack and thus no longer provide WSN with adequate security from this attack. Furthermore, the detection of node clone attack in mobile WSN is far different and more challenging than in static WSNs.

High level security issues are basically identical to the security requirements of both static and mobile WSNs. Thus, when dealing with security of WSNs, one is faced with achieving some of the following common security goals including availability, authenticity, confidentiality, and data integrity. When node clone attack is launched by an adversary, all of these security goals are affected severely because of two reasons. First, if any proper, specific, and efficient detection scheme is not used to identify and revoke these clones because the existing general purpose security protocols would allow the clone nodes to encrypt, decrypt, and authenticate all of their communications as if they were original captured nodes. Second, when the detection probability of the detection technique used is very low to detect these clones or clones. Node clone attack is significantly harmful to the networks because these clones or clones have legitimate keys, and they are recognized as legitimate members of the network, since they carry all cryptographic materials extracted from the captured nodes so that an adversary can use them to mount a variety of insider attacks [2]; for example, it can monitor all the information passing through the nodes or monitor significant fraction of the network traffic that passes through the nodes, falsify sensor data, launch denial of service (DoS) attack, extract data from the network, inject false data to corrupt the sensor's monitoring operation, subvert data aggregation, and jam legitimate signals and can also cause continual disruption to network operations by undermining common network protocols.

Availability ensures the survivability of network services despite attacks [31]. In case of node clone attack, an adversary is able to compromise the availability of WSN by launching a denial of service (DoS) attack, which can severely hinder the network's ability to continue its processing. By jamming legitimate signals, the availability of the network assets to authorized parties is also affected.

Authenticity is a security goal that enables a node to ensure the identity of the sensor node it is communicating with. In case of node clone attack, an adversary creates clone nodes which are seemingly legitimate ones (identical to the original captured node) as they have all the secret credentials of the captured node; thus, it is difficult for any node to differentiate between a clone node and the original or legitimate node. Also the existing authentication techniques cannot detect clone nodes as they all hold legitimate keys. This is how the authenticity of the network is affected.

Confidentiality is the assurance that sensitive data is being accessed and viewed only by those who are authorized to see it. But when node clone attack is launched, confidentiality of data is not assured as clone nodes are the duplicated nodes of the compromised ones, and thus they behave like original compromised nodes. These clone nodes can have all the data that contains trade secrets for commercial business, secret classified government information, or private medical or financial records, and thus by misusing such sensitive data, it can damage the network or organization, person, and governmental body.

Data integrity ensures that the contents of data or correspondences are preserved and remain unharmed during the transmission from sender to receiver. Integrity represents that there is a guarantee that a message sent is the message received meaning that it was not altered either intentionally or unintentionally during transmission. But in case of node clone attack, an adversary can falsify sensor data or can inject false data to corrupt the sensitive data and thus subverting the data aggregation using the cloned or clone nodes.

For the performance analysis and evaluation of clone detection protocols, four vital evaluation metrics are mostly used by all the detection schemes. These are communication overhead, storage or memory overhead, detection probability and detection time [26].

ISSN (Online) 2321 – 2004
ISSN (Print) 2321 – 5526

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH IN ELECTRICAL, ELECTRONICS, INSTRUMENTATION AND CONTROL ENGINEERING
Vol. 2, Issue 12, December 2014

Communication overhead is defined as the average number of messages sent by a sensor node while propagating the location claims. Storage overhead defines the average number of the location claims stored in a sensor node. Detection probability is an important evaluation metric which shows how accurately a protocol can identify and detect the clones or clones. The detection time is simply the delay between actual clone node deployment and detection.

Structure of Assessment

The association steps of this paper is as follows. The Introductory Section ends with a brief introduction of Clone Attack Detection and its necessity in Wireless sensor network. The part A in introduction shows a brief explanation about principle of Clone Attack detection in wireless sensor networks.

In Section II, explains a General review of clone attach Detection Techniques for Stationary WSNs, Many techniques have been proposed for the detection of node clone attack in static WSNs which are categorized in this section.

Section III provide the information about the review on recent researches in clone attack Detection Techniques for Mobile Wireless sensor networks. The node clone detection techniques developed for static WSNs, do not work when the nodes are expected to move as in mobile WSNs, and thus they have turned out to be ineffective for mobile WSNs. As a result some techniques have also been developed for mobile WSNs to detect the clone or clone nodes which is described in this section.

Section IV addresses the Comparison of clone attack Detection Schemes for wireless sensor networks. So far, many techniques have been proposed to detect clone attack in WSNs which are broadly categorized and compared according to used technique, their advantages and shortcomings.

Section V shows the observations, discussion and tabular comparison of different researches reviewed in previous sections. And a general conclusion of the paper, regarding review is presented in Section VI.

II CLONE ATTACK DETECTION TECHNIQUES FOR STATIONARY WIRELESS SENSOR NETWORKS

Many techniques have been proposed for the detection of clone attack in static WSNs which are categorized mainly into two types as centralized and distributed techniques. In centralized techniques base station is considered to be a powerful central which is responsible for information convergence and decision making. During the detection process every node in the network sends its location claim (ID, Location Info) to base station (sink node) through its neighboring nodes. Upon receiving the entire location claims, the base station checks the node IDs along their location, and if it finds two different locations with the same ID, it raises a clone node alarm. In distributed techniques, no central authority exists, and special detection mechanism called claimer-reporter-witness is provided in which the detection is performed by locally distributed node sending the location claim not to the base station (sink) but to a randomly selected node called witness node.

Brooks et al. [32] have proposed a cloned key detection protocol in the context of random key predistribution [33]. The basic idea is that the keys employed according to the random key predistribution scheme should follow a certain pattern, and those keys whose usage exceeds a threshold can be judged to be cloned. In the protocol, counting Bloom filters is used to collect key usage statistics. Each node makes a counting Bloom filter of the keys it uses to communicate with neighboring nodes. It appends a random number (nonce) to the Bloom filter and encrypts the result using base station public key; this encrypted data structure is forwarded to base station.

Choi et al. [23] have proposed a clone detection approach in sensor networks called SET. In SET, the network is randomly divided into exclusive subsets. Each of the subsets has a subset leader, and members are one hop away from their subset leader. Multiple roots are randomly decided to construct multiple subtrees, and each subset is a node of the subtree. Each subset leader collects member information and forwards it to the root of the subtree. The intersection operation is performed on each root of the subtree to detect cloned nodes. If the intersection of all subsets of a subtree is empty, there are no clone nodes in this subtree.

Xing et al. [34] have proposed real-time detection of clone attacks in WSN. In their approach, each sensor computes a fingerprint by incorporating the neighborhood information through a superimposed s-disjunct code [35]. Each node stores the fingerprint of all neighbors. Whenever a node sends a message, the fingerprint should be included in the message, and thus neighbors can verify the fingerprint. The messages sent by clone nodes deployed in other locations will be detected and dropped since the fingerprint does not belong to the same "community." The motivation behind their scheme for detection of clone attacks is exploring the social characteristics of each sensor. Once they are deployed, these sensors reside within a fixed neighborhood. The sensor and its neighborhood form a small "community," or a "social network."

Znaidi et al. [36] have proposed a cluster head selection-based hierarchical distributed algorithm for detecting node clone attacks using a Bloom filter mechanism including the network reactions. More precisely, the algorithm relies on a cluster head selection performed using the local negotiated clustering algorithm (LNCA) protocol [37]. Each cluster head exchanges the member node Ids through a Bloom filter with the other cluster heads to detect eventual node clones. The algorithm works in three steps. In the first step all the material required for Bloom filter computations and for cryptographic operations that will be performed in the network predistributed in each sensor node. The second step performs the cluster head election. In the third step, Bloom filter construction is performed by each cluster head, and the Bloom filter verification is performed by the other cluster heads.

Yu et al. [38] have proposed a centralized technique called compressed sensing-based clone identification (CSI) for static wireless sensor networks. The basic idea behind CSI

ISSN (Online) 2321 – 2004
ISSN (Print) 2321 – 5526

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH IN ELECTRICAL, ELECTRONICS, INSTRUMENTATION AND CONTROL ENGINEERING
Vol. 2, Issue 12, December 2014

is that each node broadcasts a fixed sensed data (α) to its one hop neighbors. Sensor nodes forward and aggregate the received numbers from descendant nodes along the aggregation tree via compressed sensing-based data gathering techniques. Base station (BS), as the root of the aggregation tree, receives the aggregated result and recovers the sensed data of the network. According to the reconstructed result, the node with the sensory reading greater than α is the clone since a non-clone node can only report the number once.

The N2NB and DM protocols are two unappealing examples proposed by Parno et al. [28]. Both of protocols received relatively less attention. In N2NB, each node floods the entire network with authenticated broadcast to claim its own location (instead of its neighbors). Each node stores the location information for its neighbors, incurring a storage cost of $d(O)$. Each node upon receiving a conflicting claim invokes a revocation procedure against the offending nodes, and eventually any clone will be cut off by all its neighbors (thus isolated from the WSN). The N2NB protocol achieves 100% detection rate as long as the broadcast reaches every node if the network size is assumed to be n and certain duplicate suppression algorithm is employed so that each node only broadcasts a given message once.

The DM protocol is a good example to illustrate the claimer-reporter-witness framework. The claimer is a node which locally broadcasts its location claim to its neighbors, each neighbor serving as a reporter, and employs a function to map the claimer ID to a witness. Then the neighbor forwards the claim to the witness, which will receive two different location claims for the same node ID if the adversary has cloned a node. One problem can occur that the adversary can also employ the function to know about the witness for a given claimer ID, and may locate and compromise the witness node before the adversary inserts the clones into the WSN so as to evade the detection.

Parno et al. [28] have introduced two more distributed algorithms for the detection of clone nodes in wireless sensor networks which are quite mature schemes as compared to DM. The first protocol is called randomized multicast (RM) which distributes location claims to a randomly selected set of witness nodes. The birthday paradox [39] predicts that a collision will occur with high probability if the adversary attempts to clone a node. Their second protocol, line-selected multicast (LSM), exploits the routing topology of the network to select witnesses for a node location and utilizes geometric probability to detect cloned nodes.

In RM, each node broadcasts a location claim to its one-hop neighbors. Then, each neighbor selects randomly witness nodes within its communication range and forwards the location claim with a probability to the nodes closest to chosen locations by using geographic routing. At least one witness node is likely to receive conflicting location claims according to birthday paradox when cloned nodes exist in the network. In LSM, the main objective is to reduce the communication costs and increase the probability of detection. Besides storing location claims in randomly selected witness nodes, the intermediate nodes for forwarding location claims can also be witness nodes. This seems like randomly drawing a line across the network, and the intersection of two lines becomes the evidence node of receiving conflicting location claims.

Bekara and Laurent-Maknavicius [40, 41] have proposed a new protocol for securing WSN against node clone attack by limiting the order of deployment using symmetric polynomial for pair-wise key establishment and defined group-based deployment model. Their scheme requires sensors to be deployed progressively in successive generations (or group). Each node belongs to a unique generation. In their scheme, only newly deployed nodes are able to establish pairwise keys with their neighbors, and all nodes in the network know the number of the highest deployed generation. Therefore, the clone nodes will fail to establish pair-wise keys with their neighbors since the clone nodes belong to an old deployed generation.

Conti et al. have proposed a randomized, efficient, and distributed protocol called RED [42, 43] for the detection of node clone attack. It is executed at fixed intervals of time and consists in two steps. In first step, a random value, $rand$ is shared between all the nodes through base station. The second step is called detection phase. In the detection phase, each node broadcasts its claim (ID and location) to its neighboring nodes. Each neighbor node that hears a claim sends (with probability p) this claim to a set of g pseudo-randomly selected network locations. The pseudo random function takes as an input ID, random number, and g.

Zhu et al. [44, 45] have proposed two distributed protocols for detecting node clone attacks called single deterministic cell (SDC) and parallel multiple probabilistic cells (P-MPC). In both protocols, the whole sensor network is divided into cells to form a geographic grid. In SDC, each node ID is uniquely mapped to one of the cells in the grid. When executing detection procedure, each node broadcasts a location claim to its neighbors. Then, each neighbour forwards the location claim with a probability to a unique cell by executing a geographic hash function [46] with the input of node ID. Once any node in the destination cell receives the location claim, it floods the location claim to the entire cell. Each node in the destination cell stores the location claim with a probability. Therefore, the clone nodes will be detected with a certain probability since the location claims of clone nodes will be forwarded to the same cell.

Fei et al. [47] have proposed a polynomial based space-time-related pairwise key pre distribution scheme (PSPP-PKPS, for short PSPP) for wireless sensor networks, which relates the keying material of a node with its deployment time and location. In PSPP, the keying material of a node can only work at its initial deployment location. If a node leaves its deployment location, its keying material will become invalid. By using this idea, their scheme provides resistance against the clone attack.

Ko et al. [48] have proposed a real time neighbour-based detection scheme (NBDS) for node clone attack in wireless sensor networks. The main idea of their scheme is that when a person moves to another community, he will

ISSN (Online) 2321 – 2004
ISSN (Print) 2321 – 5526

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH IN ELECTRICAL, ELECTRONICS, INSTRUMENTATION AND CONTROL ENGINEERING
Vol. 2, Issue 12, December 2014

meet new neighbors and tell his new neighbors where he comes from through chatting. But new neighbors will not check if he lies or not.

Ho [49] has proposed a node capture detection scheme for wireless sensor networks. Their scheme detects the captured sensor nodes by using the sequential analysis. They use the fact that the physically captured nodes are not present in the network during the period from the captured time to the redeployment time. Accordingly, captured nodes would not participate in any network operations during that period. By leveraging this intuition, the captured nodes can be detected by using the sequential probability ratio test (SPRT) [50]. The protocol first measures the absence time period of a sensor node and then compares it to a predefined threshold. If it is more than threshold value, the sensor node is considered as a captured node. The efficient node capture detection capability depends on a properly configured threshold value.

Kim et al. [56] have presented a distributed, deterministic approach to detect node clone attack. Their scheme works in three steps: initialization, witness node discovery phase, and node revocation phase. In initialization phase, before deployment, a base station (BS) associates a particular location coordinate (hereafter referred to as the verification point, vp) with each node id using geographic hash function F.

III CLONE ATTACK DETECTION TECHNIQUES FOR MOBILE WIRELESS SENSOR NETWORKS

Mobility has become an important area of research for WSN community. In mobile WSNs, mobility plays a key role in the execution of the application as the introduction of mobile entities can resolve some problems and offer many advantages over the static WSNs. The node clone detection techniques developed for static WSNs, do not work when the nodes are expected to move as in mobile WSNs, and thus they have turned out to be ineffective for mobile WSNs. As a result some techniques (still not mature enough) have also been developed for mobile WSNs to detect the clone or clone nodes.

Ho et al. [58, 59] have proposed a mobile clone detection scheme based on the sequential probability ratio test (SPRT) [50]. Their protocol is based on the fact that an uncompromised mobile node should never move at speeds in excess of the system-configured maximum speed. As a result, an uncompromised (original) mobile sensor node measured speed will appear to be at most the system-configured maximum speed as long as speed measurement system with low error rate is employed.

Deng and Xiong [60] have proposed a new protocol to detect the clones in mobile WSNs. They have used the idea of polynomial-based pair-wise key pre-distribution and Bloom Filters which insure that the clones can never lie about their real identifiers and collect the number of pair-wise keys established by each sensor node. Clones are detected by looking at whether the number of pair-wise keys established by them exceeds the threshold. The protocol works in three steps, node initialization, pair-wise establishment, and detection.

Wang and Shi [63] have employed mobile nodes as patrollers to detect clones distributed in different zones in a network, in which a basic patrol detection protocol and two detection algorithms for stationary and mobile modes are presented. The detection of clones in stationary sensors is based on the assumptions that if two or more sensors in different locations have the same ID, then all the nodes with the ID will be regarded as compromised nodes or its clones. Also, for mobile sensors (patroller), if a mobile node moves with a speed higher than the denoted maximum speed, it will be regarded as a clone attack.

Lou et al. [64] have proposed a node clone attack detection protocol, namely, the single hop detection (SHP) for mobile wireless sensor networks. The SHD protocol exploits the fact that at any time, a physical node (or equivalently, its node ID and private key) cannot appear at different neighborhood community; otherwise, there must be clones in the network. The neighborhood community of a node is characterized by its one-hop neighbor node list, which is readily available in a typical WSN since sensor nodes need to know their neighbors in order to communicate with each other.

Zhu et al. [65] have proposed two clone detection algorithms for mobile sensor networks. First algorithm is a token-based authentication scheme proposed for the detection of clone attack in which the clones do not cooperate (non-conspiring case). For the case in which the clones cooperate by communicating with each other in an efficient manner, a detection method is proposed which is based on statistics and the random encounters between physical nodes. In the first algorithm, the base station periodically broadcasts to the entire sensing region a timestamp protected by a broadcast authentication protocol. The broadcast announces the beginning of a detection round.

Conti et al. [66] have proposed two algorithms for the detection of node capture attack in mobile wireless sensor networks. Their first algorithm is simple distributed detection (SDD) in which the attack is detected using only information local to the nodes. The second algorithm is called cooperative distributed detection (CDD) which exploits node collaboration to improve the detection performance.

Deng et al. [67] have proposed two schemes for the detection of node clone attack in mobile wireless sensor networks. The first is called unary time location storage and exchange (UTLSE), and, second is called multitime location storage and diffusion (MTLSD). In both protocols, after receiving the time-location claims, witnesses carry these claims around the network instead of transmitting them. That means that data are forwarded only when appropriate witnesses encounter each other. Only if two nodes encounter each other, they exchange their time-location claims, that is, if a tracer receives a time location claim from its tracked neighbor node, it does not immediately transmit this time-location claim to the witness if the witness is not currently within its communication range but stores that location claim until encountering the witness.

ISSN (Online) 2321 – 2004
ISSN (Print) 2321 – 5526

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH IN ELECTRICAL, ELECTRONICS, INSTRUMENTATION AND CONTROL ENGINEERING
Vol. 2, Issue 12, December 2014

IV COMPARISON BETWEEN EXISTING CLONE ATTACK DETECTION APPROACHES

In this review, we have addressed an important attack on Wireless sensor network referred to as clone node attack. So far, many techniques have been proposed to detect clone attack in WSNs which is described in previous sections.

Centralized techniques are considered to be the first solutions for detecting cloned nodes which are simple but suffer from several common drawbacks. Some of the limitations of centralized techniques are found to be fairly serious like the base station which introduces a single point of failure, and any compromise of the base station will render the solution useless; also, even if there are no attacks the nodes surrounding the base station will suffer an undue communication burden which may shorten the lifetime of a network, and this approach also incurs an observable processing delay. Consequently, centralized detections have barely an advantage over distributed detections making a distributed solution a necessity.

In 2004, one of the first solutions for detecting cloned nodes was proposed by Dutertre et al., outlined in [57] which was based on a centralized base station for node clone detection. This scheme was the most straightforward one and a naive solution that provided a low defense against node clone attacks, suffering from several drawbacks as mentioned before.

In 2007, Brooks et al. [32] proposed a clone detection protocol which was based on random pairwise key pre-distribution schemes and used to tackle with detection of cloned cryptographic keys rather than clones sensor nodes. This solution seemed effective but only when the size of the keys pre-distributed to each node is small and more clones exist in the network, thus implying poor detection accuracy.

Choi et al. [23] proposed another centralized detection technique named SET in 2007 which was an attempt to reduce the detection overhead by computing set operations. But the message authentication codes used for additional security resulted in even higher detection cost in terms of computation and communication. Moreover, SET protocol is highly complex due to its complicated components, and unexpectedly an adversary can misuse the detection protocol to revoke honest nodes.

Another centralized approach was proposed in 2008 by Xing et al. [34] which used social fingerprint for the detection of clones, but it was purely based on fixed WSNs, and thus neither node addition nor disappearance can be handled. Furthermore, besides all the common limitations of centralized solutions, it cannot handle a sophisticated clone which can cleverly compute by itself a fingerprint consistent with its neighborhood in order to flee the detection at the sensor side. A more intelligent clone can dodge and avoid the detection at the base station simply by not communicating with the base station.

The most recent solution for the detection of node clone attack or clones is a centralized technique given by Yu et al. [38] in 2012. They have used a novel concept of compressed sensing for the identification of clones in the sensor network. This technique has the lowest communication overhead, but it suffers from all the common drawbacks of centralized techniques as BS is responsible for the aggregation of the result (decision) about the identification of clones in the network.

Considering the limitations of centralized detection schemes, the researchers move to a distributed solution for detecting clones, and the first naïve solution that was proposed was called node-to-network broadcasting (N2NB). Although the scheme was simple it also suffered from high memory and communication cost for large sensor networks.

Distributed techniques for the detection of clone node attack are categorized into three main classes, namely, witness node-based, neighbor-based, and generation-based or group-based techniques. All the three categories have their own pros and cons. For neighbor-based technique [48], the neighboring nodes should be static and any addition or removal of nodes is not possible throughout the detection process because in doing so the detection process is affected severely. For the generation- or group-based techniques [40, 41, 54, 55] all the nodes are deployed in groups, and no new node can be added in a particular group. Also, nodes should have location or network information before node deployment. These techniques only prevent the node clone attack but are unable to detect the clone nodes.

Zhu et al. [44, 45] proposed two techniques called single deterministic cell (SDC) and parallel multiple probabilistic cells (P-MPC) in 2007 as the variations of DM. Practically, both of these techniques depend upon the careful selection of a cell size (s) because if the cell size is too large, they incur high communication cost like N2NB, and if s is too small, it will be very easy for an adversary to trounce them by compromising all nodes in the g deterministic tiny cells. An important problem with SDC is that in order to reduce the broadcast overhead, it requires to execute the flooding only when the first copy of a node location claim arrives at the cell, and the following copies are ignored. In doing this, the node in the cell that first receives the location claim is unable to distinguish between claims of original node and clone node.

Another attempt to detect clones was made by Conti et al. [42, 43] in 2007 who have proposed a randomized, efficient, and distributed protocol named RED by combining the benefits of both DM and RM. This protocol is considered to be the most promising detection protocol which has solved the crowded center problem as the selection of witness nodes is random and fully distributed. Also, RED [4] is such an "area oblivious" protocol that associates sensor nodes with almost even responsibility, and the selection of witness nodes is pseudorandom which leads to a uniform witness distribution. Besides these advantages, the only drawback of RED is the deterministic selection of witness nodes and that the infrastructure for distributing RED's random seed may not always be available. RED is also unable to detect masked clone attack.

Bekara et al. [40, 41] in 2007 proposed a solution for preventing WSN from node clone attack which exploits the fact that excluding new nodes from joining the

ISSN (Online) 2321 – 2004
ISSN (Print) 2321 – 5526

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH IN ELECTRICAL, ELECTRONICS, INSTRUMENTATION AND CONTROL ENGINEERING
Vol. 2, Issue 12, December 2014

network can prevent clone attacks. The main drawback of this scheme is that the sensor nodes are bound to their groups and geographic locations.

A simplified version of N2NB was proposed by Zhang et al. [3] in 2009 known as randomly directed exploration (RDE). Its network communication overhead is reduced, but storage cost remains the same with N2NB. The detection rate is also decreased and may not be very significant even for a convex deployment field concluding that RDE appears to be feasible only for an ideal network model.

Another work in this area is done by Zeng et al. [4] in 2010 who have proposed two detection protocols, namely, Random Walk (RAWL) and Table-assisted Random Walk (TRAWL) for the detection of node clone attack. Both of these protocols are an extension of LSM and thus suffer from the same drawbacks. Although they have much higher detection probability than LSM, both RAWL and TRAWL require more than twice the communication overhead of LSM.

For an inclusive survey, we have also analyzed some other distributed techniques which are neither very popular nor have promising results in detecting node clone attack. These techniques include Ho et al. [54] proposed in 2009, Kim et al. [56] proposed in 2009, and Meng et al. [53] proposed in 2010.

Ho et al. [58, 59] have proposed a centralized detection scheme for mobile WSNs in which accurate measurement is a prerequisite for acceptable false-negative and -positive rates. In result, it requires dynamic and precise localization system and a tight time synchronization which are both nontrivial tasks. Also, better and accurate sampling entails even much more expensive equipment (GPS) and thus may not be affordable for the current generation of WSNs.

Another centralized detection technique is proposed by Deng and Xiong [60] in which there is no way to ensure, the participating clone node will report their keys honestly to the base station. It is possible that an original node number of pairwise keys exceed the threshold value due to its communication. Also as the effectiveness of both the above centralized detection techniques relies on the involvement of the base station, this easily incurs the problems of single-point failure and fast energy depletion of the sensor nodes around the base station.

Yu et al. [61] have proposed distributed detection technique called extremely efficient detection technique (XED) in which the authors have assumed that the clones cannot communicate and collaborate (or cooperate) with each other which is the weakness of this scheme because in case when the clones cooperate with each other, they can establish secret channels among each other, and then they can easily deceive the detection technique. Efficient and distributed detection (EDD) is another distributed detection technique for mobile WSNs proposed by Yu et al. [62] which is inapplicable due to high storage overhead for large-scale WSNs.

Zhu et al. [65] have proposed a token-based detection technique which fails when a smart attacker establishes secret channels among clones as by doing this, clones can share the tokens and make the protocol exist in name only.

Conti et al. [66] have proposed two solutions, namely, SDD and CDD for the detection of node capture. Their approach is based on a simple observation which completely assumes that there is no membership change in the network; for example, at least no nodes die out (meaning run out of power) which is not the case in reality. Also, it is assumed implicitly that any senor node is able to flood the entire mobile WSN with a broadcast message which is also not possible in reality.

V OBSERVATIONS & DISCUSSION

Node clone attack or clone attack is one of the most harmful and dangerous threat to an unattended wireless sensor network because in this attack an adversary not only compromises the sensor nodes but can also carry out a large class of internal attacks for instance DoS attack, Sybil attack, and Black hole, and wormhole attack, by surreptitiously inserting arbitrary number of clones at strategic positions of the network. Furthermore this is more niggling and troublesome because these cloned nodes, under the control of an adversary, having all the keying materials, pretend as authorized users in the network and thus deceiving the network into accepting them as legitimate nodes. It is difficult to identify clones because of two major reasons. First, since a clone or clone is considered to be completely honest by its neighbors, the legitimate nodes cannot be aware of the fact that they have a clone among them. Voting mechanisms [33, 69] remain unsuccessful to detect clone nodes that are not within the same neighborhood as a voting mechanism is used to detect misbehaving nodes and clones within the neighborhood to agree on the legitimacy of a given node. Thus, there is a need for global countermeasure that can detect clones on the global level. Second, the general purpose security protocols for secure sensor network communication would allow clone nodes to create pair-wise shared keys with other nodes and the base station, and thus in doing so, the clone nodes are able to encrypt, decrypt, and authenticate all of their communications as if they were the original captured nodes.

The process or stages of node clone attack can be described as: At Stage 1, an adversary physically captures a sensor node. After physical capture the sensor node remains absent from the network for a specific period of time. If this absence of a sensor node is detected or a tamper-proof hardware is used, the attack will be prevented. Otherwise, an attacker or an adversary starts extracting all the secret materials of the captured node at Stage 2. At Stage 3, an adversary reprograms the captured node. If an adversary is unable to use a new hardware, it can compromise the node and then exploits the compromised node to disrupt the network operations by its misbehaving activities. At Stage 4, an adversary makes clones or clones of the captured nodes by using new hardware, and these clones have the same ID and all other keying materials as that of the captured node. After making clones or clones, an adversary redeploys them at strategic positions of the network for further insider attacks at Stage 5. Finally these clones or clones can be detected by using various detection schemes.

ISSN (Online) 2321 – 2004
ISSN (Print) 2321 – 5526

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH IN ELECTRICAL, ELECTRONICS, INSTRUMENTATION AND CONTROL ENGINEERING
Vol. 2, Issue 12, December 2014

Since clone nodes carry all the cryptographic and keying materials, all the traditional authentication and intrusion detection techniques are ineffective to discover and detect these clones or clones in the network. Keeping this in mind many techniques have been proposed for the detection of node clone attack and recall that these are broadly categorized into centralized and distributed techniques. Some fairly serious limitations of centralized technique like the base station introduces a single point of failure, and any compromise of the base station will make the solution useless thus making distributed solutions a necessity. One important class of distributed techniques is witness node-based techniques which are considered to the most favorable techniques yet for detecting clone nodes. But according to Zeng et al. [4], clone detection protocols must be non-deterministic and fully distributed in order to circumvent the existing drawbacks of witness-based strategies. The witness node-based strategies ought to fulfill three requirements to have a high probability of detecting clones or clones. Firstly, the selection of witness-nodes should be nondeterministic as it is more difficult for an adversary to launch clone attacks in nondeterministic protocols successfully because the witnesses of node are not known and are different in each execution of the protocol. Secondly, for any given node, all the nodes should have an equal probability to be the witnesses of that node during the lifetime of the network. Thirdly, the witness-nodes should be selected from all over the network randomly and not from particular area of the network every time meaning that the witness distribution should be uniform throughout the entire network.

There are two types of attacks which are the variations of node clone attack and can be launched by an adversary against witness node-based schemes. These are named as smart attack and masked clone attack. Smart attack is a special witness compromising attack, and in this attack an adversary avariciously chooses which sensor to corrupt in order to maximize its chance for its clones to go undetected. The adversary finds out the witness nodes which are used to detect clones and only compromises these witness nodes to avoid detection. The witness node-based techniques use a framework called claimer-reporter-witness framework in which a node referred to as claimer, locally broadcasts it location claim to its neighbors. Each neighbor serves as a reporter and employs a function to map the claimer ID to a witness. The neighbor forwards the claim to the witness and if it receives two different location claims for the same node ID then it means that the adversary has cloned a node. The adversary can also employ a function to know about the witness for the given claimer ID, and may also locate and compromise the witness node before she inserts the clones into the wireless sensor network in order to evade the detection. In masked clone attack, the adversary may turn to compromise all the neighbors of a clone so as to prevent a location claim from propagating to any witness thus eliminating the reporters at all.

Nowadays, mobility has become an important area of research for WSN community. In mobile WSNs, mobility plays a key role in the execution of the application [68] as the integration of mobility in WSN can improve the coverage and utility of the sensor network deployment and enables more versatile sensing applications as well. However, besides that the introduction of mobile entities (which freely roam in the network and are autonomous as being able to reposition and organize themselves in the network) can resolve some problems by offering many advantages over the static WSNs the unique properties of mobile WSNs and the dynamic mobile network topology pose many new challenges in the security of mobile WSNs. The idea of detecting clone nodes in static WSNs is extensively based on the elitism of the node location meaning that a sensor node should be allied to a unique deployment position, and if one logical node id is found to be associated with two or more physical locations, the node clone is detected. But noticeably this is not applicable to the emerging mobile WSNs where the sensor nodes are moving freely all the time in the network. Thus, a little work (which includes significantly different scenarios and techniques) has been done so far to deal with clones or clones in mobile WSNs.

VI CONCLUSION

This paper reviewed the state-of-the-art schemes for detection of node clone attack also called clone attack. The existing techniques are broadly categorized into two classes distributed and centralized. Both classes of schemes are proficient in detecting and preventing clone attacks, but both schemes also have some noteworthy drawbacks. However, to sum up, the current study highlights the fact that there are still a lot of challenges and issues in clone detection schemes that need to be resolved to become more applicable to real-life situations and also to become accepted by the resource constrained sensor node.

A. Tabular Comparison on Some Surveyed Literatures

Author	Research	Description
Sathish, R.	Dynamic Detection of Clone Attack in Wireless Sensor Networks	There are few distributed solutions available for this problem. But the issues related to energy and memory demanding in any WSN protocol makes these solutions ineffective. In order to overcome these drawbacks, a lightweight, fast, efficient and mobile agent based security solution against cloning attack or replication attack is been proposed for WSNs.
Wen, H.	Lightweight and effective detection scheme for node clone attack in wireless sensor networks	A novel scheme to detect the node clone attack in WSN by channel identification characteristic is presented, in which the clone nodes are distinguished by the channel responses between nodes. The proposed scheme aims at achieving fast detection and minimising

		the data transmission cost by taking advantage of temporal and spatial uniqueness in physical layer channel responses.
Kai Xing	Real-Time Detection of Clone Attacks in Wireless Sensor Networks	Previous works against clone attacks suffer from either a high communication/storage overhead or a poor detection accuracy. This paper propose a novel scheme for detecting clone attacks in sensor networks, which computes for each sensor a social fingerprint by extracting the neighborhood characteristics, and verifies the legitimacy of the originator for each message by checking the enclosed fingerprint.
Yingpei Zeng	Random-walk based approach to detect clone attacks in wireless sensor networks	This paper first show that in order to avoid existing drawbacks, replica-detection protocols must be non-deterministic and fully distributed (NDFD), and fulfil three security requirements on witness selection. To our knowledge, only one existing protocol, Randomized Multicast, is NDFD and fulfils the requirements, but it has very high communication overhead. Then, based on random walk, we propose two new NDFD protocols, RAndom WaLk (RAWL) and Table-assisted RAndom WaLk (TRAWL), which fulfil the requirements while having only moderate communication and memory overheads.
Conti, M.	Distributed Detection of Clone Attacks in Wireless Sensor Networks	A serious drawback for any protocol to be used in the WSN-resource-constrained environment. Further, they are vulnerable to the specific adversary models introduced in this paper. The contributions of this work are threefold. First, analyse the desirable properties of a distributed mechanism for the detection of node replication attacks. Second, show that the known solutions for this problem do not completely meet our requirements. Third, propose a new self-healing, Randomized, Efficient, and Distributed (RED) protocol for the detection of node replication attacks, and we show that it satisfies the introduced requirements.
Yanzhi Ren	Social closeness based clone attack detection for mobile healthcare system	Existing clone attack mitigation approaches either only focus on the prevention techniques or can only work in static or well-connected networks, and hence are not applicable to our targeted mobile healthcare systems. This paper propose a social closeness based method in a mobile healthcare disease control system to detect any clone attacks that may be launched to disrupt the normal operations of the system. This social closeness based method exploits the social relationships among users for clone attack detection.
Kwantae Cho	Classification and Experimental Analysis for Clone Detection Approaches in Wireless Sensor Networks	First investigate the selection criteria of clone detection schemes with regard to device types, detection methodologies, deployment strategies, and detection ranges. We then classify the existing schemes according to the proposed criteria. Simulation experiments are conducted to compare their performances. It is concluded that it is beneficial to utilize the grid deployment knowledge for static sensor networks; the scheme using the grid deployment knowledge can save energy by up to 94.44% in comparable performance.
Sheela, D.	Efficient approach to detect clone attacks in Wireless sensor networks	An increasing body of protocols has been proposed in recent years for detecting node replication attack in sensor networks. Most of them however expose the following limitations: high performance overheads, unreasonable assumptions, necessity of central control, lack of smart attack detection etc. To address these issues, author propose two new protocols in this paper: Random Witness Selection (RWS) Protocol & Minimized Random Witness Selection (MRWS) protocol which fulfill the requirements while having only moderation communication and memory overheads.
Zheng, Zhongming	ERCD: An energy-efficient clone detection protocol in WSNs	This paper, propose a location-aware clone detection protocol, which guarantees successful clone attack detection and has little negative impact on the network lifetime. Specifically, we utilize the location information of sensors and randomly select witness nodes located in a ring area to verify the privacy of sensors and to detect clone attacks. The ring structure facilitates energy efficient data forwarding along the path towards the witnesses and the sink, and the traffic load is distributed across the network, which improves the network lifetime significantly.
Brooks, R.	On the Detection of Clones in Sensor Networks Using Random Key Predistribution	This paper propose an algorithm that a sensor network can use to detect the presence of clones. Keys that are present on the cloned nodes are detected by looking at how often they are used to authenticate nodes in the network. Simulations verify that the proposed method accurately detects the presence of clones in the system and supports their removal.

Udgata, S.K.	Wireless Sensor Network Security Model Using Zero Knowledge Protocol	This paper, address some of the special security threats and attacks in WSNs. Author propose a scheme for detection of distributed sensor cloning attack and use of zero knowledge protocol (ZKP) for verifying the authenticity of the sender sensor nodes. The cloning attack is addressed by attaching a unique fingerprint to each node that depends on the set of neighboring nodes and itself.
Manivannan, D.	An efficient authentication protocol based on congruence for Wireless Sensor networks	The proposed protocol uses Fermat Number Theorem (FNT) and Combinations of Chinese Remainder Theorem with Fermat Numbers (CRT_FN) to enhance the strength of authentication mechanism among the sensor Nodes. In between Node to Node authentication FNT is used, Cluster head to Node and Base station to Cluster head CRT_FN is used. Comparison of the proposed protocol with existing protocols is done.
Heesook Choi	SET: Detecting node clones in sensor networks	This paper, propose a new effective and efficient scheme, called SET, to detect such clone attacks. The key idea of SET is to detect clones by computing set operations (intersection and union) of exclusive subsets in the network. First, SET securely forms exclusive unit subsets among one-hop neighbors in the network in a distributed way.
Zhijun Li	Randomly directed exploration: An efficient node clone detection protocol in wireless sensor networks	This paper, propose an innovative randomly directed exploration protocol to detect the node clone. Each node need only know its neighbours' information, and then collaborates to forward claiming messages, trying to find out clone. No any specific routing protocols or infrastructures are demanded in the proposed protocol. Therefore, it is highly practical in the general sensor network applications. In addition, the memory requirement of the protocol is almost optimal.
Ming Zhang	Memory Efficient Protocols for Detecting Node replication attacks in wireless sensor networks	This paper, propose four replication detection protocols that have high detection probability, low memory requirement, and balanced energy consumption. The new protocols use Bloom filters to compress the information stored at the sensors, and use two new techniques, called cell forwarding and cross forwarding, to improve detection probability, further reduce memory consumption, and in the meantime distribute the memory and energy overhead evenly across the whole network.

REFERENCES

[1] T. Bonaci, P. Lee, L. Bushnell, and R. Poovendran, "Distributed clone detection in wireless sensor networks: an optimization approach," in Proceedings of the 2nd IEEE International Workshop on Data Security and Privacy in Wireless Networks (WoWMoM '11), Lucca, Italy, June 2011.

[2] W. T. Zhu, J. Zhou, R. H. Deng, and F. Bao, "Detecting node replication attacks in wireless sensor networks: a survey," Journal of Network and Computer Applications, vol. 35, no. 3, pp. 1022–1034, 2012.

[3] M. Zhang, V. Khanapure, S. Chen, and X. Xiao, "Memory efficient protocols for detecting node replication attacks in wireless sensor networks," in Proceedings of the 17th IEEE International Conference on Network Protocols (ICNP '09), pp. 284–293, Princeton, NJ, USA, October 2009.

[4] Y. Zeng, J. Cao, S. Zhang, S. Guo, and L. Xie, "Random walk based approach to detect clone attacks in wireless sensor networks," IEEE Journal on Selected Areas in Communications, vol. 28, no. 5, pp. 677–691, 2010.

[5] R. Di Pietro, L. V. Mancini, C. Soriente, A. Spognardi, and G. Tsudik, "Data security in unattended wireless sensor networks," IEEE Transactions on Computers, vol. 58, no. 11, pp. 1500–1511, 2009.

[6] C. Karlof and D. Wagner, "Secure routing in wireless sensor networks: attacks and countermeasures," in Proceedings of the 1st IEEE International Workshop on Sensor Network Protocols and Applications, May 2003.

[7] B. Parno, M. Luk, E. Gaustad, and A. Perrig, "Secure sensor network routing: a cleanslate approach," in Proceedings of the ACM CoNEXT Conference (CoNEXT '06), December 2006.

[8] F. Ye, H. Luo, S. Lu, and L. Zhang, "Statistical en-route filtering of injected false data in sensor networks," in Proceedings of the IEEE INFOCOM, 2004.

[9] L. Yu and J. Li, "Grouping based resilient statistical en-route filtering for sensor networks," in Proceedings of the IEEE INFOCOM, 2009.

[10] S. Zhu, S. Setia, S. Jajodia, and P. Ning, "An interleaved hop-by-hop authentication scheme for filtering of injected false data in sensor networks," in Proceedings of the IEEE Symposium on Security and Privacy, pp. 259–271, May 2004.

[11] H. Chan, A. Perrig, and D. Song, "Secure hierarchical in-network aggregation in sensor networks," in Proceedings of the13th ACM Conference on Computer and Communications Security (CCS '06), pp. 278–287, November 2006.

[12] J. Deng, R. Han, and S. Mishra, "Security support for in network processing in wireless sensor networks," in Proceedings of the ACM Workshop on Security in Ad Hoc and Sensor Networks (SASN '03), pp. 83–93, 2003.

[13] B. Przydatek, D. Song, and A. Perrig, "SIA: secure information aggregation in sensor networks," in Proceedings of the 1st International Conference on Embedded Networked Sensor Systems (SenSys '03), pp. 255–265, November 2003.

[14] Y. Yang, X. Wang, S. Zhu, and G. Cao, "SDAP: a secure hop-by-hop data aggregation protocol for sensor networks," in Proceedings of the 7th ACM International Symposium on Mobile Ad Hoc Networking and Computing (MOBIHOC '06), pp. 356–367, May 2006.

[15] S. Capkun and J. P. Hubaux, "Secure positioning in wireless networks," IEEE Journal on Selected Areas in Communications, vol. 24, no. 2, pp. 221–232, 2006.

[16] S. Ganeriwal, S. Čapkun, C. C. Han, and M. B. Srivastava, "Secure time synchronization service for sensor networks," in Proceedings of the ACM Workshop on Wireless Security (WiSe '05), pp. 97–106, September 2005.

[17] X. Hu, T. Park, and K. G. Shin, "Attack tolerant time synchronization in wireless sensor networks," in Proceedings of the 27th IEEE Conference on Computer Communications (INFOCOM '08), pp. 41–45, Phoenix, Ariz, USA, April 2008.
[18] Z. Li, W. Trappe, Y. Zhang, and B. Nath, "Robust statistical methods for securing wireless localization in sensor networks," in Proceedings of the 4th International Symposium on Information Processing in Sensor Networks (IPSN '05), pp. 91–98, April 2005.
[19] D. Liu, P. Ning, and W. Du, "Attack-resistant location estimation in sensor networks," in Proceedings of the 4th International Symposium on Information Processing in Sensor Networks (IPSN '05), pp. 99–106, April 2005.
[20] H. Song, S. Zhu, and G. Cao, "Attack resilient time synchronization for wireless sensor networks," Ad Hoc Networks, vol. 5, no. 1, pp. 112–125, 2007.
[21] K. Sun, P. Ning, C. Wang, A. Liu, and Y. Zhou, "TinySeRSync: secure and resilient time synchronization in wireless sensor networks," in Proceedings of the 13th ACM Conference on Computer and Communications Security (CCS '06), pp. 264–277, 2006.
[22] C. Hartung, J. Balasalle, and R. Han, "Node compromise in sensor networks: the need for secure systems," Tech. Rep. CU-CS-988-04, Department of Computer Science, University of Colorado at Boulder, 2004.
[23] H. Choi, S. Zhu, and T. F. L. Porta, "SET: detecting node clones in sensor networks," in Proceedings of the 3rd International Conference on Security and Privacy in Communication Networks (SecureComm '07), pp. 341–350, September 2007.
[24] S. Gautam Thakur, "CINORA: cell based identification of node replication attack in wireless sensor networks," in Proceedings of the IEEE International Conference on Communications Systems (ICCS '08), 2008.
[25] S. Hussain and M. S. Rahman, "Using received signal strength indicator to detect node replacement and replication attacks in wireless sensor networks," in Data Mining, Intrusion Detection, Information Security and Assurance, and Data Networks Security 2009, vol. 7344 of Proceedings of SPIE, April 2009.
[26] J. Yick, B. Mukherjee, and D. Ghosal, "Wireless sensor network survey," Computer Networks, vol. 52, no. 12, pp. 2292–2330, 2008.
[27] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, "Wireless sensor networks: a survey," International Journal of Computer and Telecommunications Networking, vol. 38, no. 4, pp. 393–422, 2002.
[28] B. Parno, A. Perrig, and V. Gligor, "Distributed detection of node replication attacks in sensor networks," in Proceedings of the IEEE Symposium on Security and Privacy (IEEE S and P '05), pp. 49–63, May 2005.–213, May 2003.
[29] A. Seshadri, A. Perrig, L. van Doorn, and P. Khosla, "SWATT: softWare-based attestation for embedded devices," in Proceedings of the IEEE Symposium on Security and Privacy (IEEE S and P '04), pp. 272–282, May 2004.
[30] R. D. Pietro, L. V. Mancini, C. Soriente, A. Spognardi, and G. Tsudik, "Catch me (If you can): data survival in unattended sensor networks," in Proceedings of the 6th Annual IEEE International Conference on Pervasive Computing and Communications (PerCom '08), pp. 185–194, March 2008.
[31] F. Hu and N. K. Sharma, "Security considerations in ad hoc sensor networks," Ad Hoc Networks, vol. 3, no. 1, pp. 69–89, 2005.
[32] R. Brooks, P. Y. Govindaraju, M. Pirretti, N. Vijaykrishnan, and M. T. Kandemir, "On the detection of clones in sensor networks using random key predistribution," IEEE Transactions on Systems, Man and Cybernetics C, vol. 37, no. 6, pp. 1246–1258, 2007.
[33] 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, pp. 41–47, Washington, DC, USA, November 2002.
[34] K. Xing, X. Cheng, F. Liu, and D. H. C. Du, "Real-time detection of clone attacks in wireless sensor networks," in Proceedings of the 28th International Conference on Distributed Computing Systems (ICDCS '08), pp. 3–10, Beijing, China, July 2008.
[35] K. Xing, X. Cheng, L. Ma, and Q. Liang, "Superimposed code based channel assignment in multi-radio multi-channel wireless mesh networks," in Proceedings of the 13th Annual ACM International Conference on Mobile Computing and Networking (MobiCom '07), pp. 15–26, September 2007.
[36] W. Znaidi, M. Minier, and S. Ubeda, "Hierarchical node replication attacks detection in Proceedings of the 20th IEEE Personal, Indoor and Mobile Radio Communications Symposium (PIMRC '09), pp. 82–86, Tokyo, Japan, September 2009.
[37] D. Xia and N. Vlajic, "Near-optimal node clustering in wireless sensor networks for environment monitoring," in Proceedings of the 21st International Conference on Advanced Networking and Applications (AINA '07), pp. 632–641, IEEE Computer Society, Washington, DC, USA, 2007.
[38] C. M. Yu, C. S. Lu, and S. Y. Kuo, "CSI: compressed sensing-based clone identification in sensor networks," in Proceedings of the IEEE International Conference on Pervasive Computing and Communications Workshops (PERCOM Workshops '12), pp. 290–295, Lugano, Switzerland, March 2012.
[39] A. J. Menezes, S. A. Vanstone, and P. C. V. Orschot, Handbook of Applied Cryptography, CRC Press, New York, NY, USA, 1996.
[40] C. Bekara and M. Laurent-Maknavicius, "A new protocol for securing wireless sensor networks against nodes replication attacks," in Proceedings of the 3rd IEEE International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob '07), White Plains, NY, USA, October 2007.
[41] C. Bekara and M. Laurent-Maknavicius, "Defending against nodes replication attacks on wireless sensor networks," 2012,
[42] M. Conti, R. Di Pietro, L. V. Mancini, and A. Mei, "A randomized, efficient, and distributed protocol for the detection of node replication attacks in wireless sensor networks," in Proceedings of the 8th ACM International Symposium on Mobile Ad Hoc Networking and Computing (MobiHoc '07), pp. 80–89, September 2007.
[43] M. Conti, R. Di Pietro, L. Mancini, and A. Mei, "Distributed detection of clone attacks in wireless sensor networks," IEEE Transactions on Dependable and Secure Computing, vol. 8, no. 5, pp. 685–698, 2011.
[44] B. Zhu, V. G. K. Addada, S. Setia, S. Jajodia, and S. Roy, "Efficient distributed detection of node replication attacks in sensor networks," in Proceedings of the 23rd Annual Computer Security Applications Conference (ACSAC '07), pp. 257–266, Miami Beach, Fla, USA, December 2007.
[45] B. Zhu, S. Setia, S. Jajodia, S. Roy, and L. Wang, "Localized multicast: efficient and distributed replica detection in large-scale sensor networks," IEEE Transactions on Mobile Computing, vol. 9, no. 7, pp. 913–926, 2010.
[46] S. Ratnasamy, B. Karp, L. Yin et al., "GHT: a geographic hash table for data-centric storage," in Proceedings of the 1st ACM International Workshop on Wireless Sensor Networks and Applications (WSNA '02), pp. 78–87, September 2002.

BIOGRAPHIES

Manjunatha R C obtained his B.E and M.Tech Degree from Visveshwaraya University, Karnataka, India, in 2006 and 2008 respectively in Telecommunication Engineering. He is working as Assistant professor at Acharya Institute of Technology, Bangalore, and Karnataka. He is currently pursuing his Ph.D at Jain University, Karnataka. His current research includes Clone detection in wireless Sensor Networks.

Dr K. R. Rekha obtained her ME degree from Bangalore University, India in 2000. She is working as a Professor in the Department of Electronics and Communication in SJB Institute of Technology, Bangalore. she has pursued her Ph. D. degree in Dr MGR University, Chennai. Her research interests include Wireless communication, FPGA implementation, and Microcontroller and Embedded systems design. She is a member of MIE, MISTE and IETE

Dr K. R. Nataraj obtained his ME degree from Bangalore University, India in 2000. He worked as Professor and Head of the Department during 2000-2008 and currently he is the Post Graduate Coordinator in the Department of Electronics and Communication in SJB Institute of Technology, Bangalore. Presently, His research interests include Wireless communication, FPGA implementation, and Microcontroller and Embedded systems design. He is a member of MIE, MISTE , IETE and IEEE