ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 5, Special Issue 4, February 2018

DETECTION OF CLONE ATTACKS IN WIRELESS SENSOR NETWORKS

M.SILAMBARASI,
M.M.E.S WOMEN'S ARTS AND SCIENCE COLLEGE, MELVISHRAM.
Simbu_arasi@yahoo.com

R.SANGEETHA,
M.M.E.S WOMEN'S ARTS AND SCIENCE COLLEGE, MELVISHRAM.
oviyasangeetha80@gmail.com

ABSTRACT

A Wireless Sensor Network is a set of sensors that communicate through wireless links. Wireless Sensor Networks is used in a wide range of applications such as environmental tracking, target tracking, health monitoring, smart homes, surveillance system, military applications etc. Each node in Wireless Sensor Networks composed of a micro-sensor with the capacity of acquisition, processing and by data transmission. The sensor nodes usually deploy in geographic locations to keep track of changes in the environment. Some kind of attacks might occur to the nodes or the data transferred between the nodes. The security of operations within a Wireless Sensor Network requires the protection of messages exhausted between the sensor nodes. One such challenge to the sensor network is the clone attack or the node replication attack. In order to detect and prevent the Clone attack, different approaches are used. Considering, the challenges in the Wireless Sensor Network, a trust based Clone detection approach is used to identify the cloned node in the network.

Keywords: Wireless Sensor Networks, Security Requirements, Security Attacks, Clone Attack Detection Schemes.

I. INTRODUCTION

In recent years an efficient design of a Wireless Sensor Network has become a leading area of research. A Sensor is a device that responds and detects some type of input from both the physical or environmental conditions, such as pressure, heat, light, etc. The output of the sensor is generally an electrical signal that is transmitted to a controller for further processing.

A Wireless sensor network can be defined as a network of devices that can communicate the information gathered from a monitored field through wireless links.

A Wireless Sensor Network is one kind of wireless network includes a large number of circulating, self-directed, minute, low powered devices named sensor nodes called motes. These networks certainly cover a huge number of spatially distributed, little, battery-operated, embedded devices that are networked to caringly collect, process, and transfer data to the operators, and it has controlled the capabilities of computing & processing. Nodes are the tiny computers, which work jointly to form the networks. These are similar to wireless ad hoc networks in the sense that they rely on wireless connectivity and spontaneous formation of networks so that sensor data can be transported wirelessly.

WSN is spatially autonomous sensors to monitor physical or environmental conditions, such as temperature, sound, pressure, etc. and to cooperatively pass their data through the network to main locations. It is mainly used for Industrial and Consumer Applications to monitor their process.

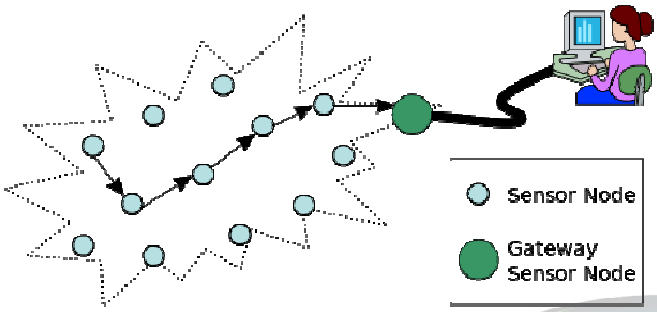
II. WIRELESS SENSOR NETWORK ARCHITECTURE

The Wireless Sensor Network is built of "nodes", where each node is connected to one (or sometimes several) sensors. Each node has a Radio Transceiver with an internal antenna or connection to an external antenna, a Microcontroller, an electronic circuit for interfacing with the sensors and an energy source. Size and cost constraints on sensor nodes result in corresponding constraints on resources such as energy, memory, computational speed and communications bandwidth. The topology of the Wireless Sensor Networks can vary from a simple star network to an advanced multi-

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 5, Special Issue 4, February 2018

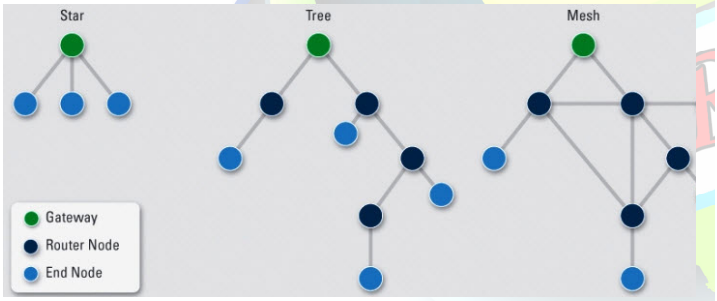
hop wireless mesh network. The propagation technique between the hops of the network can be routed or flooding.



Typical multi-hop wireless sensor network architecture

III. WIRELESS SENSOR NETWORK TOPOLOGIES

Wireless Sensor Network has various topologies like the ones given below.



Wireless Sensor Network Topologies

Star Topologies

Star topology is a communication topology, where each node connects directly to a gateway. A single gateway can send or receive a message to a number of remote nodes. In star topologies, the nodes are not permitted to send messages to each other. This allows low-latency communications between the remote node and the gateway (base station).

Due to its dependency on a single node to manage the network, the gateway must be within the radio transmission range of all the individual nodes. The advantage includes the ability to keep the remote nodes' power consumption to a minimum and simply under control. The size of the network depends on the number of connections made to the hub.

Tree Topologies

Tree topology is also called as cascaded star topology. In tree topologies, each node connects to a node that is placed higher in the tree, and then to the gateway. The main advantage of the tree topology is that the expansion of a network can be easily possible, and also error detection becomes easy. The disadvantage with this network is that it relies heavily on the bus cable; if it breaks, all the network will collapse.

Mesh Topologies

The Mesh topologies allow transmission of data from one node to another within its radio transmission range. If a node wants to send a message to another node, which is out of radio communication range, it needs an intermediate node to forward the message to the desired node. The advantage with this mesh topology includes easy isolation and detection of faults in the network. The disadvantage is that the network is large and requires huge investment.

IV. TYPES OF WIRELESS SENSOR NETWORK

Different types of Wireless Sensor Networks include

1. Terrestrial WSNs
2. Underground WSNs
3. Underwater WSNs
4. Multimedia WSNs
5. Mobile WSNs

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 5, Special Issue 4, February 2018

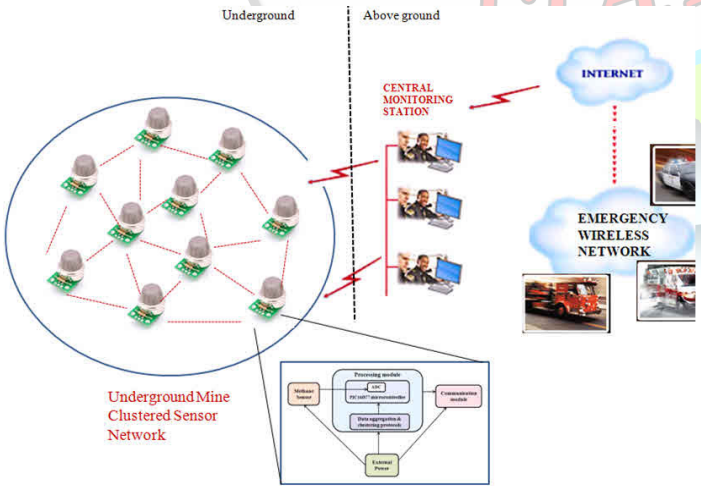
1. Terrestrial WSNs

Terrestrial WSNs are capable of communicating base stations efficiently, and consist of hundreds of thousands of wireless sensor nodes deployed either in unstructured (ad hoc) or structured (Pre planned) manner. In an unstructured mode, the sensor nodes are randomly distributed within the target area that is dropped from a fixed plane. The pre planned or structured mode considers optimal placement, grid placement, and 2D, 3D placement models.

In this Wireless Sensor Network, the battery power is limited; however, the battery is equipped with solar cells as a secondary power source. The Energy conservation of this Wireless Sensor Network is achieved by using low duty cycle operations, minimizing delays, and optimal routing, and so on.

2. Underground WSNs

The underground wireless sensor networks are more expensive. The Wireless Sensor Network networks consist of a number of sensor nodes that are hidden in the ground to monitor underground conditions. To relay information from the sensor nodes to the base station, additional sink nodes are located above the ground.

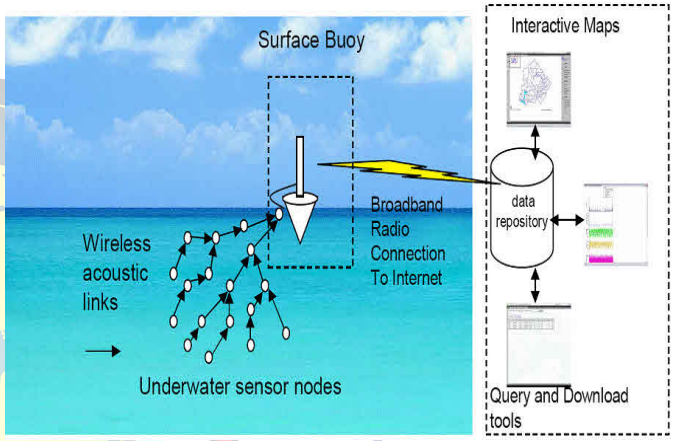


Underground WSNs

The underground wireless sensor networks deployed in the ground are difficult to recharge. The sensor battery nodes equipped with a limited battery power are difficult to recharge. In addition to this, the underground environment makes wireless communication a challenge due to high level of attenuation and signal loss.

3. Under Water WSNs

More than 70% of the earth is occupied with water. These networks consist of a number of sensor nodes and vehicles deployed under water. Autonomous underwater vehicles are used for gathering data from these sensor nodes. A challenge of underwater communication is a long propagation delay, and bandwidth and sensor failures.



Under Water WSNs

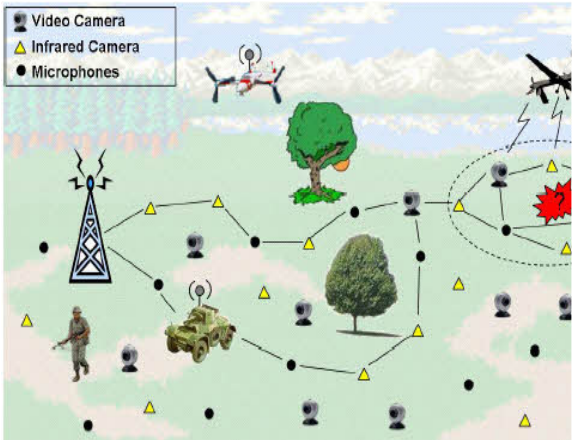
Under water WSNs are equipped with a limited battery that cannot be recharged or replaced. The issue of energy conservation for underwater WSNs involves the development of underwater communication and networking techniques.

4. Multimedia WSNs

Multimedia wireless sensor networks have been proposed to enable tracking and monitoring of events in the form of multimedia, such as imaging, video, and audio. These networks consist of low-cost sensor nodes equipped with microphones and cameras. These nodes are interconnected with each other over a wireless connection for data compression, data retrieval and correlation.

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 5, Special Issue 4, February 2018



Multimedia WSNs

The challenges with the multimedia WSN include high energy consumption, high bandwidth requirements, data processing and compressing techniques. In addition to this, multimedia contents require high bandwidth for the contents to be delivered properly and easily.

5. Mobile WSNs

These networks consist of a collection of sensor nodes that can be moved on their own and can be interacted with the physical environment. The mobile nodes have the ability to compute sensed and communicate. The mobile wireless sensor networks are much more versatile than the static sensor networks.

Security

Security plays a vital role to defend against various types of attacks on wireless sensor networks. To protect the information and resources from attacks is the main goal of security services. The basic security requirements are:

- **Availability:**
  It ensures that services should be available by WSN whenever it is required.
- **Authorization:**
  It guarantees that the only legal sensor can provide information to the network.
- **Authentication:**
  It empowers a node to guarantee the identity of neighbour to which it is communicating.
- **Confidentiality:**
  It makes sure that only authorized sensor node is accessing the content of messages.
- **Integrity:**
  It measures that received data has not been modified by an adversary.
- **Freshness:**
  It makes sure that no old messages have been repeated.

V. SECURITY ATTACKS ON WSN

There are a number of attacks on Wireless Sensor Networks. Let us explain it one by one as follows:-

Sinkhole Attack: The main goal of an adversary in sinkhole attack is to attract all the traffic to itself through an agreement node. Sinkhole attacks typically work by making a compromised node look especially attractive to surrounding nodes. [4]

- **Wormhole Attack:** In wormhole attack, packets are recorded by an attacker at one location, and then attacker tunnels them into another location and again transmits them into the network. In figure 3, packets established by node X are replayed through the node Y and vice-versa.

- **Selective Forward Attack:** In this attack, an attacker comprises itself in a data stream lane and can selectively drop only distinct packets. In sensor networks, it is assumed that nodes faithfully forward received messages but some compromised node might refuse to forward packets, though neighbours may start using another route.

Sybil Attack: In Sybil attack, a single node makes replicas of it and distributes it in multiple locations of the network. Authentication and encryption techniques can prevent an outsider to launch a Sybil attack on the sensor network. [4]

- **Hello Flood Attack:** In this type of attack, an attacker with high energy and a high radio transmission range broadcasts HELLO packets to a numerous nodes in the network and then these sensor nodes are influenced that adversary is their neighbour. Due to this an injured node ultimately deceived by an attacker.

- **Clone Attack:** Here the attacker will capture a node and extract its cryptographic secrets and make a copy of this node in the entire networks due to this an attacker can easily move the packets.

- **Denial of Service:** Denial of Service (DoS) is created by the accidental crash of nodes or wicked

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 5, Special Issue 4, February 2018

action. DoS attack is intended not only for the enemy's attempt to threaten, interrupt, or destroy a network, but also for any incident that diminishes a network's potential to distribute a service

• **False Node:** In this attack an adversary add a spiteful node to the network which generates a false data in the network. This kind of attack is one of the dangerous attacks which can destroy the whole of the network.

• **Message Corruption:** Any modification of the content of a message by an attacker compromises its integrity [6].

• **Physical Attack:** Unlike other attacks, physical attacks obliterate sensors eternally.

VI. NEIGHBOR BASED DETECTION SCHEME (NBDS)

Usually everyone lives in a community and probably knows their neighbors. For some reasons we might move to another city and live in another community. Our idea is that when a person moves to another community, she will meet new neighbors and tell her new neighbors where she comes from through chatting. But new neighbors will not check if she lies or not. However, if some of her new neighbors ask her previous neighbors whether this newcomer really comes from the community that she claims, the identity of newcomer can be implicitly verified. If previous neighbors say that this person still lives in the original neighborhood, the newcomer can be detected as a replica. This observation motivates our research on node replication attacks. We describe the detail of NBDS below.

A. *Description of NBDS*

When a node i moves to another location (node i might be a clone node or legitimate node), node i should broadcast a rejoining claim to its new neighbors for rejoining the network. The format of the rejoining claim is

$$[Rejoin, ID_i, <neighbor\text{-}list>_{pre}, SIG_{SKi}(H(Rejoin \| ID_i \| <neighbor\text{-}list>_{pre}))] \quad (1)$$

where *Rejoin* indicates this is a rejoining claim, $\|$ denotes the concatenation operation and $<neighbor\text{-}list>_{pre}$ denotes IDs of all previous neighbors of node i. Upon receiving the rejoining claim, each new neighbor first verifies the signature. If the signature verification is passed, each new neighbor independently forwards the rejoining claim with a probability pf to a randomly selected node from $<neighbor\text{-}list>_{pre}$ and set a timer T_{join}.

Once the rejoining claims arrive at destination nodes, the nodes receiving the rejoining claim first verify the validity of the signature, and then check if ID_i is in the neighbor table. If ID_i is not in the neighbor table, the nodes receiving the rejoining claim send a report to the BS for handling this problem. The reason for sending the report to the BS is that node i may lie about $<neighbor\text{-}list>_{pre}$. The BS may then send a revocation message of node i after receiving the report.

If ID_i is in the neighbor table of nodes receiving the rejoining claim, it means nodes receiving the rejoining claims from node i's new neighbors are really node i's previous neighbors. Next, nodes receiving the rejoining claim check if node i still exists in this neighborhood by sending a one-hop challenge message encrypted with the key shared with node i. If node i still exists in this neighborhood, node i will response an existence claim for challenge message. The format of the existence claim is

$$[Existence, ID_i, <neighbor\text{-}list>_{cur}, SIG_{SKi}(H(Existence \| ID_i \| <neighbor\text{-}list>_{cur}))] \quad (2)$$

, where *Existence* indicates this is an existence claim and $<neighbor\text{-}list>_{cur}$ denotes IDs of all node i's current neighbors. Once receiving the existence claim from node i, previous neighbors of node i verify the signature. If the signature is verified successively, previous neighbors of node i detect node replication attacks (the rejoining claim conflicts with the existence claim). Previous neighbors that receiving both the rejoining claim and the existence claim broadcast revocation message by using both claims as evidence to revoke node i.

If previous neighbors that sending one-hop challenge message does not receive the existence

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 5, Special Issue 4, February 2018

claim from node *i*, they send an encrypted remove-node message to all nodes in <*neighbor-list*>$_{pre}$. Each node that receiving the remove-node message will remove node *i* from their neighbor table, and not to communicate with node *i* until node *i* successively rejoins them. Note that if nodes in <*neighbor-list*>$_{pre}$ receive the rejoining claims from node *i*'s new neighbors after receiving the remove-node message, the challenge messages for node *i* will not need to be sent.

When the timer T_{join} expired, node *i*'s new neighbors accept node *i* as a legitimate node and record ID_i in their neighbor table if they do not receive any revocation message from one of nodes in <*neighbor-list*>$_{pre}$ or the BS. In the future, if node *i* again moves to another location, node *i* will broadcast a rejoining claim containing new neighbor list to the next new neighbors. Fig. 1 shows the network view of NBDS, where two dotted big circles denote the communication range of a node, two filled small circles denote target nodes and the lines from right side to left side denote the transmissions of rejoining clams from some new neighbors to some previous neighbors.

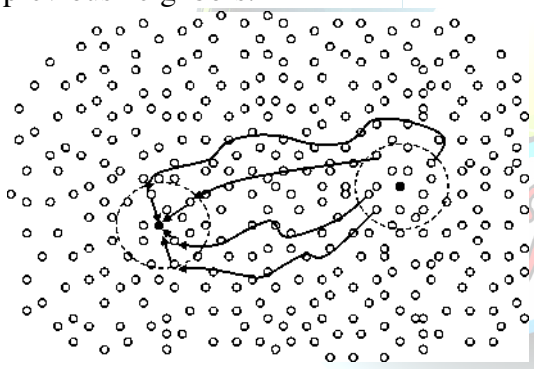


Figure 1. The network view of NBDS.

VII. ANALYSIS OF NBDS

A. *Security Analysis*

We first discuss the normal condition, i.e. no replication attacks occur and the node legitimately joins another location within the network. Node i leaves original location, and original neighbors of node i still record IDi in their neighbor table. When node i joins another location, it broadcasts a rejoining claim to its new neighbors and theses new neighbors verify the rejoining claim. Then each new neighbor independently forwards the rejoining claim to a randomly selected node from previous neighbors with a probability pf. Each previous neighbor receiving the rejoining claim checks if node i still exist in the same neighborhood by sending a one-hop challenge message. In this case, node i has already left the original location. So node i will not response the existence claim for challenge message. All previous neighbors then remove IDi from their neighbor table. When timer Tjoin set in each new neighbor of node i expired, new neighbors accept node i as a legitimate node in their neighborhood. [10] discussed about a system,the effective incentive scheme is proposed to stimulate the forwarding cooperation of nodes in VANETs. In a coalitional game model, every relevant node cooperates in forwarding messages as required by the routing protocol. This scheme is extended with constrained storage space. A lightweight approach is also proposed to stimulate the cooperation.

Considering if a replicated node, say node i', tries to join the network. Node i' will be detected since node i has to response an existence claim to its neighbors. Otherwise node i will be removed by its neighbors. So each neighbor of node i receiving both the rejoining claim and the existence claim will send a revocation message to the whole network. Both replicated node i' and node i will be revoked. Note that each neighbor of node i' forwards the rejoining claim to one of nodes in <neighbor-list>pre with a probability pf. So we would like to compute the probability of detection. In NBDS, in order to detect the node replication attacks, at least one neighbor node of node i' must forward the rejoining claim. In other words, forwarding only one rejoining clam is enough to detect node replication attacks. Therefore, the probability of detection can be easily calculated as Pdetect = 1 – (1 – pf)d and the corresponding results with pf = 0.1 and 0.2 are shown in Fig. 3.

We also consider if the replicated node i' sending a fake <neighbor-list>pre in the rejoining claim in order to avoid checking the existence of node i. However, nodes receiving the rejoining claim will check if IDi' is in the neighbor table. In this case, since node i' is not a neighbor of nodes in <neighbor-list>pre, nodes receiving the rejoining claim will send an encrypted report to the BS for handling this problem.

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 5, Special Issue 4, February 2018

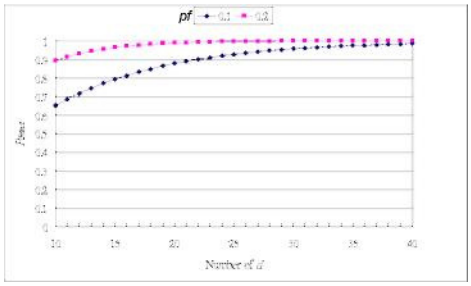


Figure 3. The probabilty of detection.

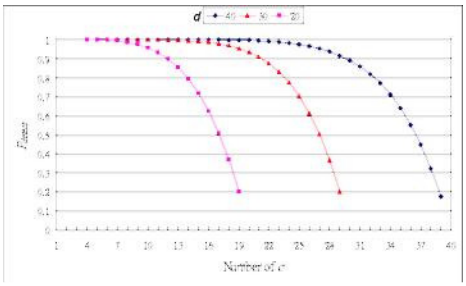
The BS may send a revocation message of $ID_{i'}$ (i.e., ID_i) after receiving this report.

We consider if $<neighbor\text{-}list>_{pre}$ contains IDs that do not exist in the network. The rejoining claims will not be sent to the previous neighbors, hence bypassing the checking procedure. However, this flaw could be easily avoided by asking acknowledgments from previous neighbors when they receiving rejoining claims. If any new neighbor forwarding rejoining claims to previous neighbor does not receive acknowledgment from previous neighbor, new neighbor will send an encrypted report to the BS for handling this problem.

If the adversary compromises some nodes in $<neighbor\text{-}list>_{pre}$, the compromised nodes will not send the challenge message to node i. However, according to our assumptions, the adversary cannot compromise all nodes in $<neighbor\text{-}list>_{pre}$. Hence, NBDS still has some probability to detect node replication attacks. We first calculate the expected number of nodes in $<neighbor\text{-}list>_{pre}$ that will receive the rejoining claim in (3).

$$E[d_{receive}] = d - ((1- dY^{pf} \cdot d)$$

Then we assume the number of nodes in $<neighbor\text{-}list>$ that have been compromised p_r



by the adversary is where $d > c \geq E[d_{receive}]$. Note that if $c < E[d_{receive}]$, the adversary cannot compromise all nodes that receive the rejoining claim. Therefore, the probability of detection when c numbers of nodes in $<neighbor\text{-}list>_{pre}$ are compromised can be calculated as in (4). Fig. 4 plots the corresponding results with pf =0.2 and d = 20, 30 and 40. As shown in Fig, with d = 20, the probability of detection is 0.6244 even if the adversary compromises 16 nodes in $<neighbor\text{-}list>_{pre}$. With d = 40, the probability of detection is 0.6393 even if the adversary compromises 35 nodes in $<neighbor\text{-}list>_{pre}$.

$$1 \quad C(d\text{-}E[d_{receive}], c\text{-}E[d_{receive}])\ C(d,c)$$

TABLE II. COMPARISONS OF COMMUNICATION AND MEMORY COSTS

	Communication	Memory
Randomized Multicast [2]	$O(n^2)$	$O(4n)$
Line-Selected Multicast [2]	$O(n \cdot 4n)$	$O(4n)$
RED [3]	$O(r \cdot yfn)$	$O(r)$
SDC [4]	$O(r \cdot 4n) + O(s)$	w
P-MPC [4]	$O(r \cdot 4n) + O(s)$	w
SET [5]	$O(n)$	N/A
NBDS	$O(r \cdot 4n)$	$O(r)$

B. Performance Analysis

We evaluate the efficiency of NBDS in terms of communication and memory costs. Note that the cost for pare-wise key establishment is eliminated since every secure WSN should adopt at least one of key establishment protocols for encrypting transmitted data. The cost for forwarding the rejoining claim to previous neighbors and the cost for each previous neighbor that receiving the rejoining claim to send a challenge message are c_{pre}, $O(d \cdot pf \cdot 4n)$ and $O(d \cdot pf)$ respectively. Obviously, only the previous neighbors that receiving the rejoining claim need to temporarily store the rejoining claim. NBDS has the memory overhead of $O(d \cdot pf)$. Table II lists the efficiency comparisons between NBDS and previous schemes [2, 3, 4, and 5]. Note that we do not compare with the schemes that only suitable for all static wireless sensor networks [6, 7] (we have already explained the drawbacks of these schemes in Section 2). We set $r = d \cdot pf$ for simplicity. S denotes the number of nodes in a cell and w denotes the number of witness nodes that stores the location claim in a cell [4].

Unfortunately, the message length of the

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 5, Special Issue 4, February 2018

rejoining claim in NBDS is longer than that of location claim used by previous schemes [2, 3, and 4] due to the neighbor list is included in the rejoining claims. For example, if each node's ID is 2 bytes, a rejoining claim requires additional $d \cdot 2$ bytes for storing neighbor list. However, we would like to emphasize that the proposed scheme is performed only once when a node moves to another location. Unlike previous schemes that periodically execute the protocol for detecting replicated nodes. We believe that NBDS still has much lower overheads.

C. New Nodes Joining

The system administrator may want to replace old nodes with new nodes for some reasons. This arises a new problem in NBDS since new nodes does not have previous neighbors. In this case, we assume the system administrator knows IDs of some neighbors of the newly deployed node. Suppose a new node j wants to join the network, node j is then pre-installed a joining claim by the system administrator. When deploying node j into the network, node j broadcasts the joining claim to its neighbors. The format of the joining claim is

$$[Join, ID_j, <neighbor\text{-}list>, Counter, SIG_{SKBS}(H(Join \| ID_j \| <neighbor\text{-}list> \| Counter))] \quad (5)$$

, where *Join* indicates this is a joining claim, <*neighbor-list*> denotes IDs of some neighbors of node j and *Counter* is a incremental counter for all new joining nodes (e.g., the tenth new deployed node has *Counter* = 10). Note that the joining claim will be received by all nodes in <*neighbor-list*>. Upon receiving the joining claim, each node checks if its ID is included in <*neighbor-list*>. If not, it just ignores the joining claim. Otherwise, it verifies the signature of the joining claim. If signature verification is passed and the value of *Counter* is greater than previous recorded value, each node accepts node j as a legitimate neighbor.

We consider if node j is compromised, the joining claim for node j is retrieved and loaded into replicated nodes by the adversary. The replicated nodes cannot join other locations since the usage of the joining claim is limited by <*neighbor-list*> and the nodes not included in <*neighbor-list*> will ignore the joining claim. We then consider if replicated nodes try to join the original location. However, nodes in <*neighbor-list*> will not accept the joining claim since the *Counter* indicates the joining claim is replayed. Nodes only accept the value of *Counter* that greater than previous recorded value.

VIII. CONCLUSION

In this paper we propose a Neighbor-Based Detection Scheme (NBDS) for detecting node replication attacks. The analysis shows NBDS achieves higher probability of detection and lower communication and memory costs than previous schemes. Even if some nodes are compromised, NBDS still provides higher probability of detection. Furthermore, NBDS achieves near real-time detection of node replication attacks. In the future, we would like to do more experiments, including the time to detect replicated nodes and comparison with previous related work in terms of communication and memory costs.

REFERENCES

[1] "Smart Dust, U C Berkeley".

[2] "An Ultra-Low Energy Microcontroller for Smart Dust Wireless Sensor Networks, ISSCC 2004"(PDF).

[3] "Emerging Challenges: Mobile Networking for "Smart Dust" by Joseph M. Kahn, Randy Howard Katz, and Kristofer S. J. Pister".

[4] Dargie, W. and Poellabauer, C. (2010). Fundamentals of wireless sensor networks: theory and practice. John Wiley and Sons. pp. 168–183, 191–192. ISBN 978-0-470-99765-9.

209. ISBN 978-0-471-74300-2.

[5] Sohraby, K., Minoli, D., Znati, T. (2007). Wireless sensor networks: technology, protocols, and applications. John Wiley and Sons. pp. 203–

[6] Peiris, V. (2013). "Highly integrated wireless sensing for body area network

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 5, Special Issue 4, February 2018

applications". SPIE Newsroom. doi:10.1117/2.1201312.005120.

[7] Tony O'Donovan; John O'Donoghue; Cormac Sreenan; David Sammon; Philip O'Reilly; Kieran A. O'Connor (2009). A Context Aware Wireless Body Area Network (BAN) (PDF). Pervasive Computing Technologies for Healthcare, 2009. doi:10.4108/ICST.PERVASIVEHEALTH2009.5987.

[8] Bilal, Muhammad; et al. "An Authentication Protocol for Future Sensor Networks".

[9] J.K.Hart and K.Martinez, "Environmental Sensor Networks: A revolution in the earth system science?", Earth Science Reviews, 2006

[10] Christo Ananth, M.Muthamil Jothi, A.Nancy, V.Manjula, R.Muthu Veni, S.Kavya, "Efficient message forwarding in MANETs", International Journal of Advanced Research in Management, Architecture, Technology and Engineering (IJARMATE), Volume 1,Issue 1, August 2015,pp:6-9.

[11] L. Doherty, K. S. J. Pister, and L. E. Ghaoui. "Convex position estimation in wireless sensor networks", *In Proceedings of 20th Annual Joint Conference of the IEEE Computer and Communications Societie* (INFOCOM), 2001.

[12] J. Newsome and D. Song. "GEM: Graph embedding for routing and data-centric storage in sensor networks without geographic information", *In Proceedings of ACM Conference on Embedded Networked Sensor Systems* (SenSys), 2003.

[13] B. Karp and H. T. Kung. "GPSR: Greedy perimeter stateless routing for wireless networks", *In Proceedings of the 6th Annual International Conference on Mobile Computing and Networking* (*MobiCom*), 2000.

[14] A. J. Menezes, S. A. Vanstone and P. C. V. Orschot. "Handbook of applied cryptography", CRC Press, Inc., 1996.

[15] S. Ratnasamy, B. Karp, L. Yin, F. Yu, D. Estrin, R. Govindan, and S. Shenker. "GHT: A geographic hash table for data-centric storage", *In Proceedings of the 1st ACM International Conference on Wireless Sensor Networks and Applications* (*WSNA*), 2002.

[16] 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 International Conference on Mobile Computing and Networking* (MobiCom), 2007.

[17] Florian Hess. "Efficient identity based signature schemes based on pairings", *In Proceedings of the 9th Annual International Workshop on Selected Areas in Cryptography* (SAC), 2002.

[18] D.Malan, M.Welsh, and M. Smith. "A public-key infrastructure for key distribution in TinyOS based on elliptic curve cryptography", *In Proceedings of 1st IEEE International Conference on Sensor and Ad hoc Communications and Networks* (*SECON*), 2004.