Chien, D.C., Ku, C.Y. & Huang, S.R. (2017). Replication attach detection in mobile wireless sensor network with LEACH-ME routing protocol. In *Proceedings of The Seventeenth International Conference on Electronic Business* (pp. 208-214). ICEB, Dubai, UAE, December 4-8.

Replication Attack Detection in Mobile Wireless Sensor Network with LEACH-ME Routing Protocol

Da-Chun Chien, National Chiao Tung University, Taiwan, jt12282575@gmail.com
Cheng-Yuan Ku*, National Chiao Tung University, Taiwan, cooper.c.y.ku@gmail.com
Shu-Rong Huang, National Chiao Tung University, Taiwan, hsr.long@gmail.com

ABSTRACT

Because the Wireless Sensor Network (WSN) nodes are low-cost devices, attackers may capture some nodes in this network and then duplicate these nodes to eavesdrop the transmitted messages or even control the network gradually without difficulty. This is the so-called node replication attack. This type of attacks could cause the huge threat to information security of WSNs. Therefore, in this paper, we would like to suggest a detection approach which can offer good performance but with higher energy consumption. Hence, it can provide an alternative solution for some specific applications that need better precision but do not care energy or lifespan too much.

Keywords: Mobile Wireless Sensor Network, Network Security, Node Replication Attack Detection, LEACH-ME Routing Protocol, Performance Evaluation.

*Corresponding author

INTRODUCTION

The WSN is composed of many wireless sensor nodes. This kind of network is often used in various scenarios such as battlefield, animal detection, sea water temperature collection, etc. Wireless sensor nodes could be self-configuring and self-maintaining with mobility or not. Furthermore, WSN nodes are often made with low-cost and less-security consideration because the deployment of WSN may need thousands of sensor nodes or more most of the time. For some particular applications, sensor nodes are also deployed in the huge open space so it may be very difficult in general to guarantee the safety of each node. These situations results in various kinds of threats to the secure operation of WSN.

Due to the characteristics of WSN, it may suffer from many kinds of attacks such as sinkhole attack, Sybil attack, wormhole attack, node replication attack and so on (Padmavathi & Shanmugapriya, 2009; Wang *et al*., 2006). Even though most of threats and attacks can be effectively prevented by using cryptographic algorithms; however, they are not suitable for WSNs due to the lightweight design of sensor nodes. In this paper, we would like to focus on node replication attack and provide a solution. As for node replication attack, the malicious attackers can capture one sensor node and then duplicate this node with many copies easily. These nodes can be deployed within the huge WSN and finally eavesdrop important messages transmitted in the network. Therefore, how to detect the node replication attack becomes one of the most important issues for information security of WSNs. Considering the potential damage caused by node replication attack, the suitable detection methods are really necessary for the future development of applications of WSN. There are lots of replication node detection approaches that had been proposed in the past. However they may only function well in different environments. Some methods work better for static nodes and some others can just be used for centralized infrastructure with superior performance. Nevertheless, we believe there is still room for improvement.

Because the transmission route of each node is different, the uneven energy dissipation may cause the lifetime decrease of WSN node. Therefore the Low-Energy Adaptive Clustering Hierarchy (LEACH) routing protocol was proposed to reduce the energy dissipation for longer use of nodes (Heinzelman *et al*., 2000). LEACH is a cluster-based routing protocol with the major consideration of saving energy; therefore, nodes are not always in the active state. Furthermore, LEACH protocol was initially designed for static nodes. In general, static nodes are easier to handle but mobile nodes play well than static nodes for many new applications. Hence, in this paper, we propose the node replication detection method based on LEACH-Mobile-Enhanced (LEACH-ME) protocol introduced in Kumar *et al*. (2008). The main purpose is to balance the energy consumption and detection rate. We believe quite a few particular applications are tolerant of some sacrifices of power consumption in return for higher detection rates.

LITERATURE REVIEW

Previous Solutions for Replication Attack

In the beginning, most of node replication detection methods relied on the Base Station (BS) to execute the centralized detection algorithms. Each node sends identification information, mainly the location claim or a list of neighboring members, to the BS for investigation. Then BS checks the received information and decides if there is a replication node. If the attacking situation happens, then BS floods the warning message all over the network to revoke that node. However, this mechanism may have the following disadvantages:

1. If the BS can't work properly, then this type of methods totally fails
2. The communication cost of centralized detection is really heavy
3. BS may become the bottleneck of whole infrastructure

To overcome the shortcomings of centralized detection, some scholars proposed local detection. They used voting mechanism to verify if a node is duplicated within a neighborhood (Chan *et al*., 2003; Eschenauer & Gligor, 2002; Newsome *et al*., 2004). This mechanism does not need BS but fails to detect clones that are far away from each other. And the communication cost of this mechanism is also very high, since *n* floodings happen in the network in each iteration where *n* is the number of nodes in the WSN.

The Detection of Node Replication Attack for Static Nodes

In Parno *et al*. (2005), they proposed two protocol that could use symmetric-key cryptography to recognize clone nodes effectively rather than asymmetric-key cryptography. First one is the Randomized Multicast (RM) protocol. This protocol chooses witness randomly. Due to the large number of nodes in WSNs, it is difficult for malicious one to guess which node is the witness. When a node announces its location, its neighbor will forward the location claim to the witness. If a witness receives an ID with different location claims, this witness will flood warning message all over the network to revoke that ID. Parno *et al*. (2005) also proposed another protocol named as Line-Selected Multicast (LSM) that further lowers the communication cost. After a node announces its location claim, its neighbor forwards the location claim to the randomly chosen witness. However, the location claim will be stored in each node's buffer along the forwarding path. And the replication node should be found at the intersection of two lines as demonstrated in Figure 1.

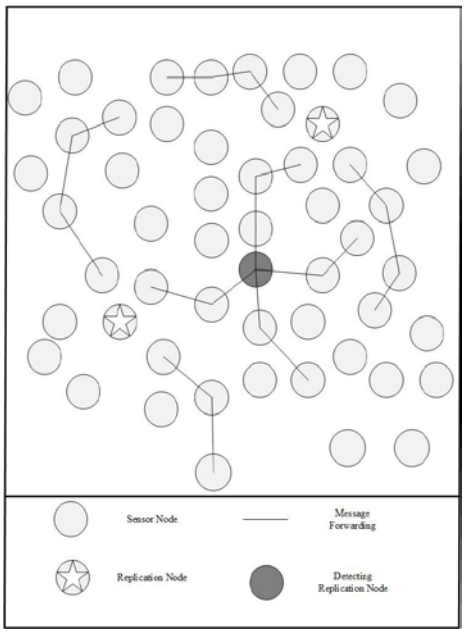

Figure 1: Replication node is detected in the intersection of two lines for LSM algorithm (Parno *et al*., 2005)

Znaidi *et al*. (2009) proposed an algorithm for detecting node replication attack in hierarchical structure WSN. Bloom filter is used in this mechanism for reducing the communication cost. This algorithm has an advantage that the length of the filter is steady but it may increase the false positive rate (FPR).

Naruephiphat *et al*. (2012) provided Area-Based Clustering Detection (ABCD) method which combines the advantages of centralized approach and clustering protocol. At the beginning, center node is chosen based on the maximum number of neighboring nodes. Then the area around the center node is separated to several sub-areas. Nodes are evenly allocated in these sub-areas and one node should be selected as witness. Each node ID and location claim must be forwarded to neighbors and then a witness but this information must pass the center node. Therefore the center node can detect replication node with two different location claim but the same ID.

Cheng *et al*. (2015) proposed a node replication detection algorithm with an improved LEACH (NI-LEACH) protocol to reduce the energy dissipation of nodes. They used a set of monitor nodes to observe the processes of data transmission in the cluster to check whether the data packet is tampered. The judgment algorithm is based on energy and covered range and NI-LEACH protocol calculates an optimal number of clusters and provides a new equation to calculate the threshold value for cluster head probability.

The Detection of Node Replication Attack for Mobile Nodes

Yu *et al*. (2013) proposed two algorithms, Extremely Efficient Detection (XED) and Efficient Distributed Detection (EDD), for detecting clone nodes in mobile WSN. The strength of these two methods is due to the localized detection, network-wide synchronization avoidance and network-wide revocation avoidance. For XED, two mobile nodes exchange a random number when they encounter each other first time. Then these two node can verify each other when they meet again. However, XED cannot protect collusion of two nodes. EDD can be used for avoiding collusion by having counters in each node to count how many times they meet each other. A threshold for these counters will be set for replication attack warning.

Another solution for mobile replication nodes detection in WSNs was proposed by Lee (2009). In this algorithm, any selected node can initiate the review round by broadcasting $R(t)$. $R(t)$ is a random number generated at time t. Any node α receives this number at time $T(\alpha)$ and this receiving time should be different for different node with very huge probability. This information with ID will be forwarded to the randomly chosen witness with probability P_λ by neighbors and the witness is responsible for replication node revocation.

PROPOSED DESIGN

To deal with the issues emphasized before, we design a node replication detection approach for mobile MSN operating on the LEACH-ME routing protocol and it is partially similar to the one proposed in Lee (2009). However, our proposed method delivers different authentication information and is working on different routing protocol. We also divide detection phase into four steps. The notations used in the detection algorithm are listed in the following Table 1.

Table 1: The notations used in the detection algorithm

Notations	Meanings
C_l	Cluster l
CH_l	Cluster head of cluster l
ID_s	ID of node s
$R(t)$	Random number generated by sink at time *t*
$T(CH_l)$	Timestamp of CH_l receiving detection request packet from sink
l_l	Member list of cluster l
m_l	Mapping list for cluster head of cluster l recording ID-timestamp pair $< ID_x, T(CH_y) >$
fi	A fixed interval for next detection cycle
$H(ID_s)$	A hash-function-based algorithm

The first step: the random number is broadcasted by sink

Detection phase is initiated by sink node in the beginning of one detection interval at time t. In general, it is often deployed around the center of WSN and is also easy to reach all of the nodes. At first, a random number $R(t)$ is generated by sink node at time t and then it uses broadcasting method to send detection request packet with $R(t)$ to all other cluster heads in the WSN as shown in Figure 2.

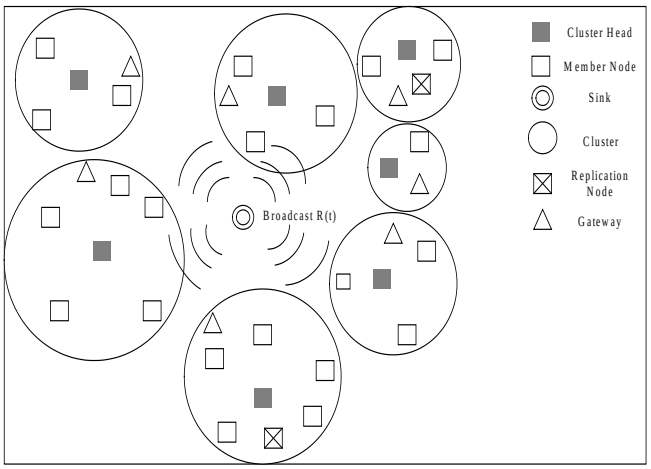

Figure 2: Broadcast of $R(t)$ from sink node to cluster nodes

The second step: is broadcasting member list.

As a cluster head CH_i receives the detection request packet, then CH_i must decide which other cluster head CH_j should be multi-casted with the verification packet that includes its member list l_i, attached $T(CH_i)$ and ID_s of cluster head CH_i.

The destination cluster head CH_j is decided by each node in the member list l_i using a well-designed hash-function-based algorithm $H(ID_s)$ which is similar to the one proposed in Lee (2009). Each node should only map into one destination cluster head. However, for the purpose of reducing communication cost, we should design the mapping algorithm with rather narrow range which only selects several destination cluster heads (two or three are better). This is another major different consideration between ours and the algorithm proposed in Lee (2009).

The third step: destination cluster head verifies all IDs in the list and timestamp in the received packet

When the cluster head CH_j receives the verification packet from CH_i, CH_j should check if the IDs in the member list l_i conflict with any ID in the ID-timestamp pair m_j : $< ID_x, T(CH_y) >$ as shown in Figure 3. If any confliction occurs, then jump to step four. If no confliction occurs, then CH_j inserts l_i and $T(CH_i)$ into m_j. After verification is done, CH_j continues to wait for new verification packets.

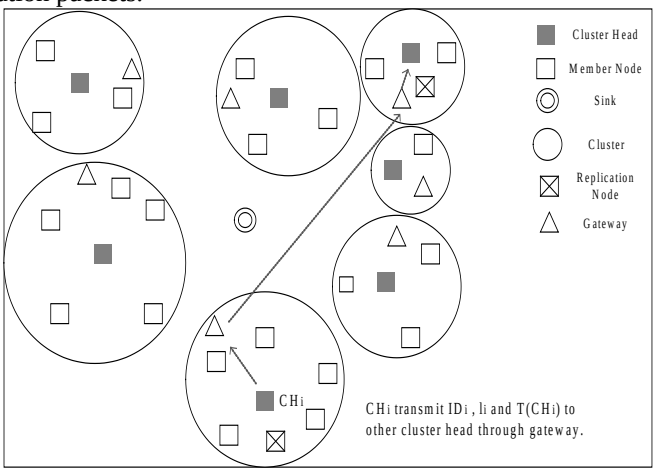

Figure 3 CH_j receives the verification packet and checks

The fourth step: cluster head broadcasts the replication node

When CH_j finds any duplicate ID, then CH_j broadcasts to other cluster heads to insert this malicious ID in the ban list and also notify all the member nodes as shown in Figure 4. This node will not be included within the information interchange network any more. After this revocation job is done, return to step 3 to continue.

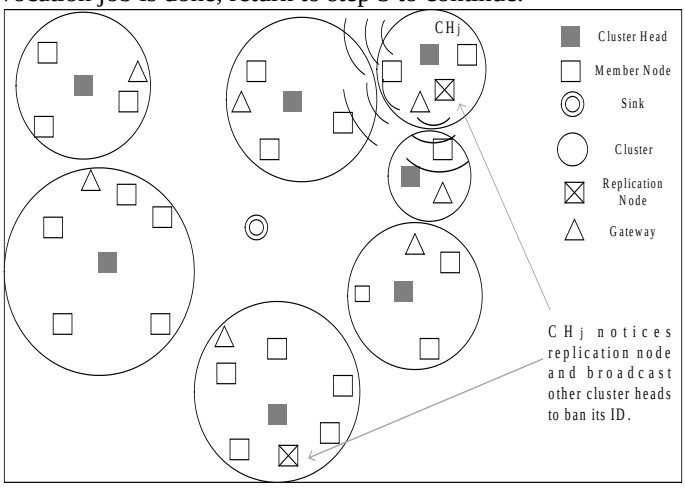

Figure 4: CH_j broadcasts to other cluster heads after detecting replication node

Sink node will start a new round of replication node detection again after a period of time fi passes, that is, will broadcast $R(t + fi)$ to initiate next round.

SIMULATION RESULTS AND DISCUSSION

Simulation Setup

We used Castalia framework as our simulation environment to evaluate energy dissipation, communication overhead and detection rates for this proposed method. Castalia is known as a famous framework for simulating WSNs and used in Boulis (2007). It is based on the popular simulator Omnet++. Omnet++ is coded in C++. Castalia has the complete radio modules of WSN and is equipped with the convenient functions for data analysis and data collection such as CastalieResult and CastaliaPlot.

Actually Castalia version 3.3 and Omnet++ version 4.6 were adopted and all the simulation parameters were set as the values demonstrated in Table 2.

Table 2: The module used and the simulation parameters

Simulation Parameters	Values
Number of nodes	400 - 1000
Simulation Time	50 sec
Field	500m * 500m
Speed	2m / sec
Detection Interval	15 seconds
E_{elec}	50 Nano Joule / bit
ε_{elec}	100 Pico Joule / bit / m^2
Repeat times	Each simulation repeats 100 times
Probability of being selected as Cluster Head	5 %
Cluster Head Rotation Interval	4 sec
TDMA slot length	0.2 sec
Radio Module	CC2420
Mobility Module	Random Waypoint

All WSN nodes except the sink were deployed randomly and uniformly in the 500 m * 500 m square field. We set all nodes except the sink node with mobility speed 2m/sec. Totally 27 replication nodes with 3 different IDs were inserted in the field for each simulation.

Results and Discussion

The following figures demonstrate the simulation results of our approach and the detection algorithm proposed in Znaidi *et al*. (2009) which is somewhat revised by us based on LEACH-ME protocol for the purpose of comparison. Our detection approach is denoted as method 1 and method 2 represents the other compared approach.

Communication Overhead

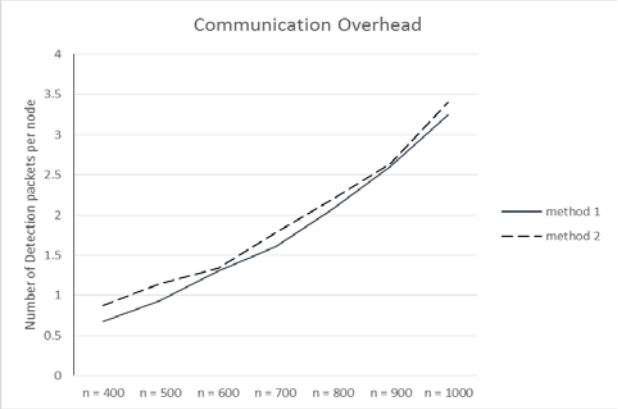

Figure 5: Comparison of communication overhead

From Figure 5, we can observe that the communication overhead of method 1 is a little bit better than method 2. However, the difference is not that significant. Furthermore, the communication cost of both methods increase exponentially with the number of nodes.

Energy Dissipation

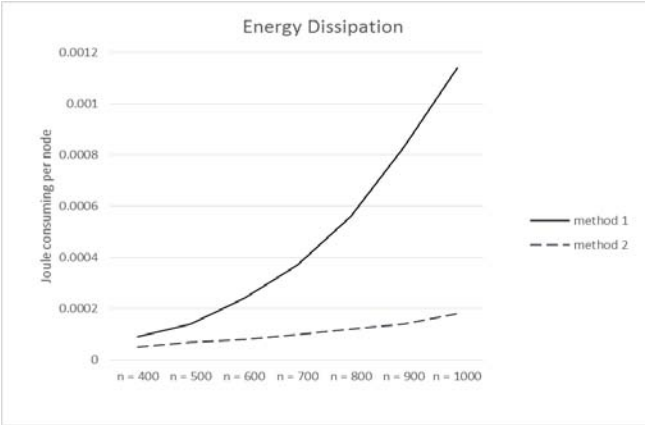

Figure 6: Comparison of energy dissipation

From Figure 6, we notice that the energy dissipation of method 2 increases smoothly; however, method 1 increases quickly. We think the better performance of method 2 is due to the adoption of Bloom filter for detection but takes the correction rate of detection as sacrifice. Bloom filter is of fixed size, so the number of necessary bits for detection does not grow with the number of nodes.

True Positive Rate (TPR)

The detection approaches of method 1 and method 2 are all based on the exchange of the member list. Hence, we cannot observe the significant difference between these two as expected according to the results in Figure 7. We also find that the TPR grows as the number of nodes. We believe that the increase of total nodes is beneficial for transmitting packets across the field even though the larger number of nodes may cause the detection more difficult.

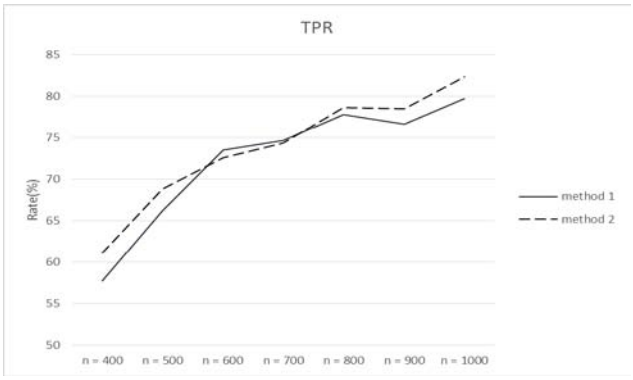

Figure 7: Comparison of true positive rates for two detection approaches

False Positive Rate (FPR)

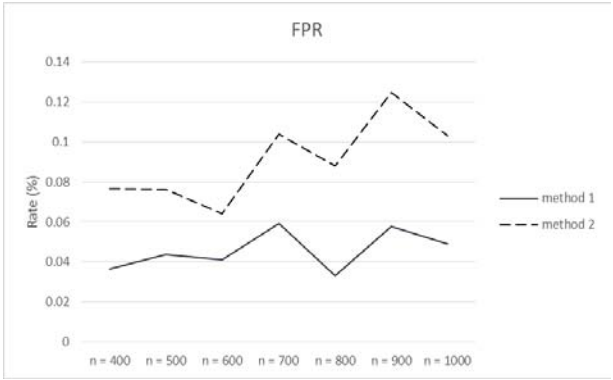

Figure 8: Comparison of false positive rate for two detection approaches

It is noticed that there is a clear gap for FPR between method 1 and method 2 as demonstrated in Figure 8. We believe it is due to the difference between detection processes. For our method, the ID of replication node is put into ban list directly but, for method 2, a cluster head needs to confirm the owner of received member list when it finds replication node ID in the Bloom filter. Because of the mobility of nodes, the confirming process of method 2 may increase the false positive rate. Moreover, these two methods have implicit but same trend as the number of nodes increases. It may be because two methods use the same original positions for each simulation even though these nodes were randomly deployed.

CONCLUSIONS

The main contribution of this paper is that we provide an alternative detection approach for node replication attack on LEACH-ME routing protocol. The primary consideration of the proposed approach is to use timestamp suggested in Lee (2009) and the member list as well but only their cluster heads are involved in the replication node detection process. Actually we believe this method can be revised slightly in the future to avoid misjudging a legal node as replication node while a node leaves one cluster but returns after just a while. Furthermore, the simulation results are provided to compare our approach with the one proposed in Znaidi *et al*. (2009) and demonstrate the useful scenarios of the proposed method. From these results, they enhance the original speculation that this approach is especially good for some particular applications which are tolerant of some sacrifices of power consumption in return for higher detection rates.

ACKNOWLEDGEMENT

This work is partially supported by MOST 106-2410-H-009-025-MY3.

REFERENCES

[1] Boulis, A. (2007, November). Castalia: revealing pitfalls in designing distributed algorithms in WSN. In *Proceedings of the 5th international conference on Embedded networked sensor systems* (pp. 407-408). ACM.

[2] Chan, H., Perrig, A., & Song, D. (2003, May). Random key predistribution schemes for sensor networks. In *Proceedings of the Symposium on Security and Privacy* (pp. 197-213). IEEE.

[3] Cheng, G., Guo, S., Yang, Y., & Wang, F. (2015, December). Replication attack detection with monitor nodes in clustered wireless sensor networks. In *IEEE 34th International Performance Computing and Communications Conference (IPCCC)* (pp. 1-8). IEEE.

[4] Eschenauer, L., & Gligor, V. D. (2002, November). A key-management scheme for distributed sensor networks. In *Proceedings of the 9th ACM Conference on Computer and Communications Security* (pp. 41-47). ACM.

[5] Heinzelman, W. R., Chandrakasan, A., & Balakrishnan, H. (2000, January). Energy-efficient communication protocol for wireless microsensor networks. In *Proceedings of the 33rd Annual Hawaii International Conference on System Sciences* Volume 8, Page 8020 (pp. 1-10). IEEE, Maui, Hawaii, January 4-7.

[6] Kumar, G. S., Vinu, P. M., & Jacob, K. P. (2008, December). Mobility metric based leach-mobile protocol. In the *16th International Conference on Advanced Computing and Communications - ADCOM 2008.* (pp. 248-253). IEEE.

[7] Lee, Yi-Chang. (2009). *A Distributed Protocol for the Detection of Node Replication Attacks in Wireless Sensor Networks*. (Master's thesis, National Chung Cheng University, Chia-Yi, Taiwan).

[8] Naruephiphat, W., Ji, Y., & Charnsripinyo, C. (2012, June). An area-based approach for node replica detection in wireless sensor networks. In *IEEE 11th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom)* (pp. 745-750). IEEE.

[9] Newsome, J., Shi, E., Song, D., & Perrig, A. (2004, April). The sybil attack in sensor networks: analysis & defenses. In *Proceedings of the 3rd International Symposium on Information Processing in Sensor Networks* (pp. 259-268). ACM.

[10] Padmavathi, D. G., & Shanmugapriya, M. (2009). A Survey of Attacks, Security Mechanisms and Challenges in Wireless Sensor Networks. *arXiv preprint arXiv:0909.0576*.

[11] Parno, B., Perrig, A., & Gligor, V. (2005, May). Distributed detection of node replication attacks in sensor networks. In , *IEEE Symposium on Security and Privacy* (pp. 49-63). IEEE.

[12] Wang, Y., Attebury, G., & Ramamurthy, B. (2006). A survey of security issues in wireless sensor networks. *IEEE Communications Surveys & Tutorials*, *8*, 2–23.

[13] Yu, C.-M., Tsou, Y.-T., Lu, C.-S., & Kuo, S.-Y. (2013). Localized algorithms for detection of node replication attacks in mobile sensor networks. *IEEE Transactions on Information Forensics and Security, 8*(5), 754-768.

[14] Znaidi, W., Minier, M., & Ubéda, S. (2009). Hierarchical node replication attacks detection in wireless sensor networks. In *Proceedings of the 20th IEEE Personal, Indoor and Mobile Radio Communications Symposium (PIMRC '09)* (pp. 82-86). IEEE, Tokyo, Japan, September 13-16.