**Journal of Computer Science 10 (8): 1473-1479, 2014**
ISSN: 1549-3636

doi:10.3844/jcssp.2014.1473.1479 Published Online 10 (8) 2014 (http://www.thescipub.com/jcs.toc)

# DETECTING MULTIPLE INTRUSION ATTACKS USING PERMANENT GIRTH CLUSTERING MODEL IN WIRELESS SENSOR NETWORK

**[1]G. Jayamurugan and [2]P. Kamalakkannan**

[1]Department of Master of Computer Applications, Sengunthar Engineering College, Tiruchengode, India
[2]Department of Computer Science, Govt. Arts College, Salem-7, India

Received 2014-02-08; Revised 2014-02-19; Accepted 2014-04-01

## ABSTRACT

Security is the central challenge and one of the serious concerns for designing reliable sensor networks. Of the different types of security threats in wireless sensor network, particularly dangerous attack is the replica node attack, in which the opponent takes the secret keying materials from a compromised node. It then produces large number of attacker-controlled replicas that divide up the cooperation node’s keying materials and ID. In this study we are specifically interested in investigating the extremely difficult problem concerning multiple attacks being routed in parallel with a given utility field and see if significant hypothetical solutions could be drawn. A clustering model for discovering multiple intrusions in WSN is identified. Permanent-girth Clustering (PC) model used to detect abnormal traffic patterns and then uses PC model to built the normal traffic behavior. In this study we develop mechanisms so that the PC model is capable to distinguish attacks. Furthermore, the detection scheme is based on position of traffic features that potentially are practical to an extensive variety of routing attacks. In order to approximate intrusion detection scheme, extensive sensor network simulator producing routing attacks in wireless sensor networks is designed. PC model for intrusion detection is capable to attain high detection accuracy with a low false positive rate for a multiplicity of replicated routing attacks. NS2 simulator is used to perform the experimental work of PC model on wireless sensor network. The experimental evaluation of PC model is measured in terms of average delay measurement, energy consumption and low false positive rate.

**Keywords:** Permanent-Girth Clustering, Wireless Sensor Network, Sequential Probability Ratio Test, Traffic Pattern, Routing Attacks

## 1. INTRODUCTION

A wireless sensor network comprises of smaller set of sensor nodes which are dispersed over the network. These nodes detect the receptive data. The base station then authenticates the data and ID which is launched by the sensor nodes which unattended that creates an opponent build many replicas. These replica nodes are unsafe in WSN.

Mobile nodes in network communication are practical for network restore and recognition. The cooperated mobile nodes insert the false data and interrupt network processes and listen in on network communications. An opponent can obtain the distinct sensor ID and build many replicas of them (Xing and Cheng, 2010).

This study explores the aforementioned techniques and integrates them together to provide a collection of intrusion attack systems in wireless sensor networks. The study is organized as follows. This study provides the necessary mechanism to provide a set of security applications in WSN. The study is presented as follows. The related works are defined in section 2. Section 3 describes the intrusion attacks problems faced by WSN, PC approach for the detection of multiple intrusion attacks. Simulation evaluation to process the PC approach is described in section 4 and the results are evaluated and discussed in section 5. Section 6 concludes the study.

**Corresponding Author:** G. Jayamurugan, Department of Master of Computer Applications, Sengunthar Engineering College, Tiruchengode, India

## 2. LITERATURE REVIEW

The connectivity present in the wireless sensor networks can be reduced to a significant rate. A, a secure connection model is designed originate from typical transmitter to the legitimate receiver over fading channels. These types of attacks based on replica node are highly susceptible as they allow the attacker to compromise certain nodes to gain control over the entire network.

Different replica node detection schemes have been presented by different researchers to mitigate those attacks. A fast and effective mobile replica node detection scheme is presented using the sequential probability ratio test. The study (Stavrou and Pitsillides, 2011) presented an interference recovery procedure in WSNs.

Wireless sensor networks are vulnerable to numerous kinds of attacks. Li *et al.* (2008), the author proposed cluster based interference detection method that divides the sensor networks into several groups.

A WSN for intrusion recognition application is proficient of noticing the physical subsistence of external intruder attacking an area beneath protection and aware the system for suitable actions (Li *et al*., 2012). A novel Cross-layer based Intrusion Detection System (CIDS) is presented in (Thamilarasu *et al*., 2005) to recognize the malevolent node(s).

A fast,efficient mobile replica node recognition method is presented in (Ho *et al*., 2009) utilizing the sequential probability ratio test. On the other hand, these systems processes on permanent sensor positions and therefore do not proceed in mobile sensor networks. Xing and Cheng (2010), the author proposed two duplication recognition systems (TDD and SDD) to undertake all these confronts from both the time and the space domain.

Zhu *et al.* (2010), a novel dispersed technique is offered as Localized Multicast for identifying the node duplication attacks. Kim *et al.* (2010), the author concerned in reducing the delay and enhancing the life span of the WSN for which procedures occur occasionally. A group of wireless networks with common intrusion constraints on the links that can be provided concurrently at specified time (Gupta and Shroff, 2010).

The relay node assignment crisis for wireless sensor networks is processed with inserting a less number of relay nodes (Misra *et al*., 2010). Yu and Yong (2010), the author presented an active filtering method that considers false insertion and DoS attacks in wireless sensor networks. Xing *et al.* (2008a), the author presented a novel method for noticing the attacks in sensor networks, which mines the neighborhood nodes and substantiates the authority of the originator.

In recent times, there has been much study on accepting the network transportation throughput of multi-hop wireless networks. To viaduct the gap in the transportation throughput among networks, the author in (La and Seo, 2011) inspected the transaction among the transportation throughput. Numerous software-based copy node recognition approaches have been proposed for static sensor networks (Xing *et al*., 2008b).

The major technique (Yu *et al*., 2009) recognizes their locations to notice contradictory reports that sign one node in numerous locations. The sensor node authentication is processed based on DDoS attacking schemes but security over the sensors is vulnerable to substantial capture attacks. This variation tends to be high false positive rate with maximum power consumption in WSN. Here, we extend this approach by defining permanent-girth clustering model in WSNs and enhance the detection accuracy efficiently and present considerably extended evaluation results, assessing not only the detection accuracy, but also minimize the power consumption of the network. In summary, our contributions are:

- To approximate intrusion detection scheme to attain high detection accuracy with a low false positive rate in wireless sensor networks
- Focuses on constructing an Intrusion Detection System for wireless sensor networks
- To explore the impact of network attacks on sensor networks using PC model based on irregularity detection
- To design an intelligent model to sense map-reading attacks that has not formerly been observed
- To attain high detection accuracy with low false positive rate for diversities of attack

## 3. DETECTING MULTIPLE INTRUSION ATTACKS USING PERMANENT GIRTH CLUSTERING MODEL

As illustrated in **Fig. 1**, we consider a two-phase approach to approximate intrusion detection scheme to attain high detection accuracy with low false positive rate in wireless sensor networks. It describes the operation of PC model from the viewpoint of a particular node, which refer to as the supervise node. In existence, all nodes are energetic in supervising the sensor network nodes using PC model.

As illustrated in **Fig. 1**, the first phase design a supervising node selects the features using four structured feature model. The second phase detects the irregularity observed in network traffic using the permanent-girth clustering model.

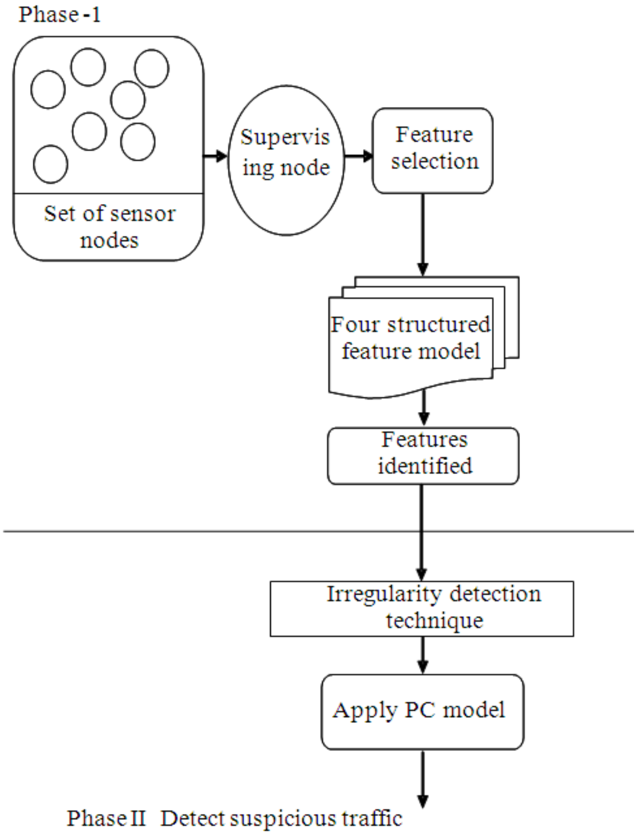

Phase -1
Set of sensor nodes
Supervising node
Feature selection
Four structured feature model
Features identified
Irregularity detection technique
Apply PC model
Phase II Detect suspicious traffic

**Fig. 1.** Flow diagram of proposed PC model

### 3.1. Problem Definition

The design considerations of PC model in wireless sensor network, comprises of set of sensor nodes S = {$s_1$,$s_2$, $s_3$ …, $s_n$} and a Base Station 'BS' so that sensors route messages to the 'BS' and vice versa. Every sensor node s € S monitors the routing messages. The routing attack is said to occur in the presence or the behavior of a compromised node denoted $s_b$ € P. The problem is for each node s € S is to identify when an attack is occurring in S.

At every time interval Ti, each sensor node constructs a characteristic vector $v_i$, which summarizes the routing information that has, been seen by that node. The feature vector $v_i$ comprises of a fixed number of attributes {$y_j$, j = 1…d}. There are two confront for intrusion detection in context. First, necessitate an effective irregularity detection scheme to detect irregular routing conditions observed in the WSN. Second, entail an appropriate set of attributes 'x' that summaries the appropriate information about the routing conditions in the network.

### 3.2. Feature Selection Using PC Model

The foremost tasks involved in PC model is to identify suitable traffic features, while attempting to have as little features as possible. This is because of the fact that higher the number of features, maximum will be the time taken to evaluate and resources desired by the nodes in the network.

Using PC model, a set of features that has to be extracted from the network traffic is seen by the supervising node as illustrated in **Fig. 2.**

The four structured features that are selected in the PC model to achieve optimality are explained below with the help of a sketch in **Fig. 3.**

The unusual levels of data traffic is detected using features relating to the number of data packet received (1). The number of route requests established (2), request sent and requests drop features. The error bit propagation (3) measures the errors received. Finally the number of updates (4) on the route to base station, mean, standard deviation of hop count to base station are intended to monitor changes regarding the path to the BS.

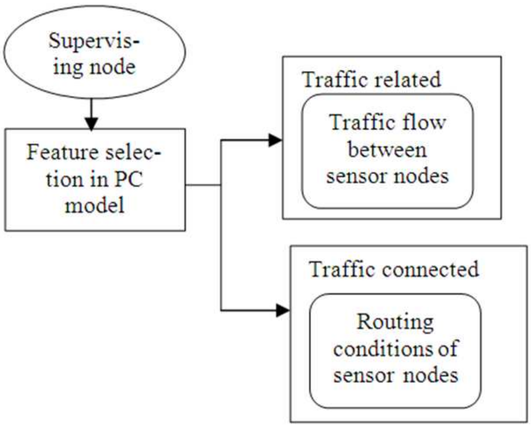

Supervis-ing node
Feature selec-tion in PC model
Traffic related
Traffic flow between sensor nodes
Traffic connected
Routing conditions of sensor nodes

**Fig. 2.** Process of feature selection in PC model

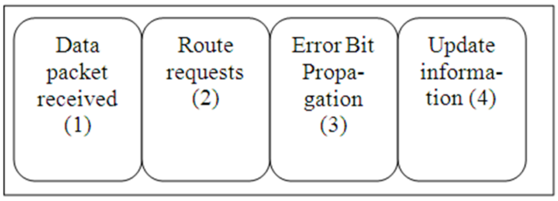


**Fig. 3.** Four structured feature model

While it is not possible to detect the authenticity of the routing packet, it is assumed that there is an amount of an attack if there is a sudden increase in the number of times the path to the base station changes compared to normal traffic conditions. The forthcoming section discusses in detail about the permanent-girth clustering model.

### 3.3. Irregularity Detection in Sensor Network Attacks

The second phase involved in detecting multiple intrusion attacks is to detect the irregularity in sensor network attacks. Detecting the reliability in PC model is to have all nodes in the sensor network independently prepared with disturbance recognition system. The major requirement of the model is that every disturbance recognition system function independently and able to detect signs of intrusion locally by observing all the data it received without collaboration between its neighbors. Each disturbance recognition system relies solely on information extracted from the node's routing table and traffic packets through the node.

### 3.4. Permanent-Girth Clustering Model

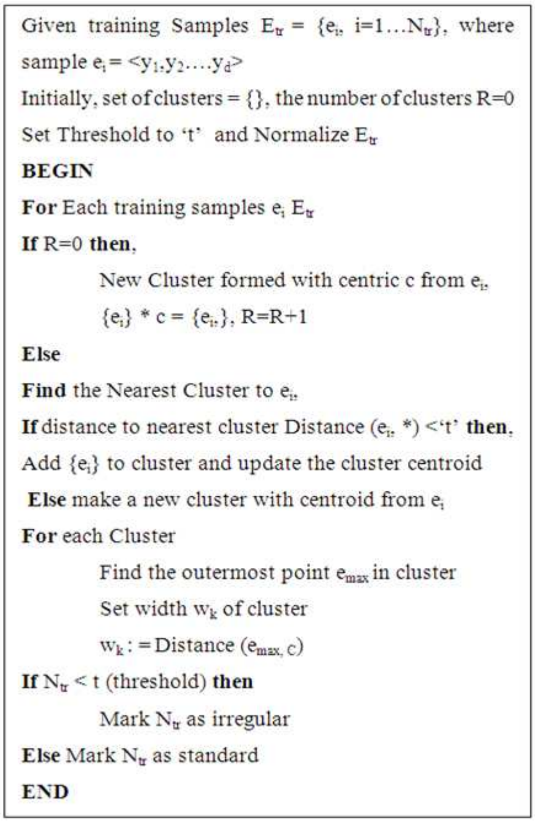
Once the features are identified, the second phase involved in the PC model is the designing of permanent-girth clustering model that detect the suspicious traffic in the network. In PC model, each sample is represented by a set of 'f' features. These features are encoded so that each sample is mapped onto a point 'e' in a feature space. The permanent-girth clustering then examines the adjacent region of the feature space for the point corresponding to that sample. If the point 'f' lies in a region of space, then label 'f' is marked as unequal. Any irregular traffic is measured to be an attack.

Equally, if 'f' lies in a solid region of space where there have been observed with many other traffic samples, then 'f' is labeled as normal. The process of irregularity detection comprises of two parts namely guidance and testing. The guidance involves the allocation of a defined set of training points. The testing analysis new network traffic samples based on the information gathered in the guidance phase. The traffic samples are then mapped to the feature space of PC model and are labeled as irregular or standard based upon the model established in the guidance part.

**Figure 4** illustrates the algorithmic process involved in building the permanent-girth clustering model. permanent-girth clustering builds a set of clusters, such that each cluster has a permanent radius in the feature space. During the guidance phase of the PC clustering model; a threshold t is chosen as the maximum radius of a cluster. The first data point forms the centric of a new cluster. If the distance of each consecutive point to its closes cluster is less than t, then the point is assigned to the cluster and the centric of the cluster is recalculated. Or else, the new peak forms the centric of a new cluster.

At the end of guidance phase, the clusters that contain less than a threshold t of the total set of points are labeled as irregular. All other clusters are labeled as standard. The testing phase operates by scheming the distance between a new point e and each cluster centric. If the distance from the experiment point e to the centric of its nearest cluster is less than w, then the new point e is known the label of the nearest cluster. If the distance from e to the adjacent cluster is greater than w, then e lies in a sparse region of the feature space and is labeled as irregular. A set of network traffic samples $E_{tr}$ for guidance, where each sample $e_i$, in this set is represented by a d-dimensional vector of attributes.

There is substantial difference in the attribute in some cases and hence, when scheming the distance between points, attributes with better values control those attributes with smaller values. Therefore to make sure that all features have the similar pressure when calculating the distance between traffic samples normalization is performed with respect to continuous attribute in terms of number of standard deviations from the mean of the attribute.



```
Given training Samples $E_{tr}$ = {$e_{i,}$ i=1…$N_{tr}$}, where sample $e_i$ = <$y_1$,$y_2$….$y_d$>
Initially, set of clusters = {}, the number of clusters R=0
Set Threshold to 't' and Normalize $E_{tr}$
BEGIN
For Each training samples $e_i$ $E_{tr}$
If R=0 then,
        New Cluster formed with centric c from $e_{i,}$
        {$e_i$} * c = {$e_{i,}$}, R=R+1
Else
Find the Nearest Cluster to $e_{i,}$
If distance to nearest cluster Distance ($e_{i,}$ *) <'t' then,
Add {$e_i$} to cluster and update the cluster centroid
 Else make a new cluster with centroid from $e_i$
For each Cluster
        Find the outermost point $e_{max}$ in cluster
        Set width $w_k$ of cluster
        $w_k$ : = Distance ($e_{max,}$ c)
If $N_{tr}$ < t (threshold) then
        Mark $N_{tr}$ as irregular
Else Mark $N_{tr}$ as standard
END
```

**Fig 4.** Permanent-girth clustering algorithm

## 4. EXPERIMENTAL EVALUATION

Our simulation scenarios are conducted with NS2 which used 25 sensor nodes, one BS and one event node. The event node represents a moving object, which is being tracked by the sensor nodes. The movement of all nodes except the base station was randomly generated over a 600×600m field, with a maximum speed of 55 m $s^{-1}$ and an average pause of 0.01 s. Each simulation was run over a time period of 1000 simulation seconds. The experimental parameter of PC model is measured in terms of average delay measurement, power consumption and low false positive rate.

## 5. RESULTS

Here we compare the performance of the proposed PC model with the existing sequential hypothesis testing for handling multiple attacks in WSN using metrics average delay, energy consumption and false positive rate.

**Figure 5** illustrates the measurement of average delay for detection of intrusion attacks in WSN. Compared to the existing sequential hypothesis testing (Ho *et al*., 2009), the average delay is lesser using the proposed PC model. **Figure 6** shows the energy consumption with comparison made to the existing sequential hypothesis testing (Ho *et al*., 2009) and finally, **Fig. 7** describes the false positive rate when compared to the existing sequential hypothesis testing (Ho *et al*., 2009), the proposed PC model has less false positive rate.

## 6. DISCUSSION

In this section (section 5), the performance of the proposed PC model is compared with the existing Sequential Hypothesis Testing for handling the multiple attacks in WSN.

**Figure 5** describes the measurement of average delay for the detection of intrusion attacks in WSN. Compared to the existing sequential hypothesis testing, the proposed PC model has less delay in detecting the presence of intrusion. This is because the proposed PC model clustered the set of sensor nodes without making a communication link between the sensor nodes in the network. So, the occurrences of the attacks over the nodes are easily identified without any further require-ments. But in the sequential hypothesis testing, time synchronization error will affect the process of identifying the intrusion attacks. The variance in the average delay is 10-15% less in the proposed PC model.

**Figure 6** describes the consumption of energy measured. Compared to the existing sequential hypothesis testing, the proposed PC model consumes less energy because the PC model identify the attacks that have not seen prior into the network. So, it does not require any communication link for detecting multiple intrusions among sensor nodes. The energy consumption by the proposed PC model performed a better packet transmission of 14-18% high as compared to the existing sequential hypothesis testing in Wireless Sensor Networks.

**Figure 7** describes the false positive rate when compared to the existing sequential hypothesis testing, the proposed PC model has less false positive rate. This is due to the fact that the proposed PC model identified the occurrence of irregularities over sensor nodes in the network and is removed immediately from the environment. The variance achieved is 12-16% better when compared to the existing sequential hypothesis testing.

Finally, it is being observed that the proposed PC model detected the abnormal traffic patterns based on a position of traffic features that potentially are practical to the different types of routing attacks.

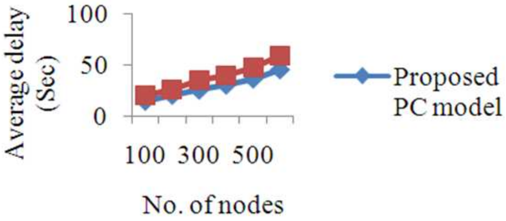


**Fig. 5.** Measure of Average delay

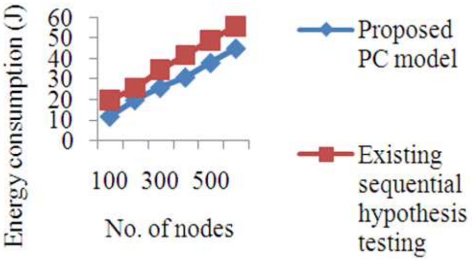


**Fig. 6.** Measure of energy consumption

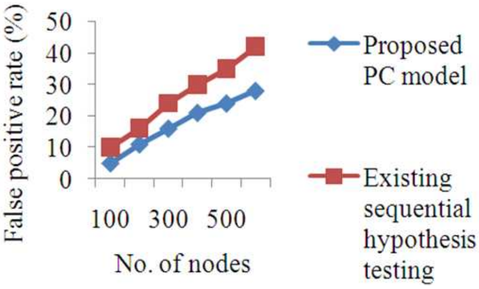


**Fig. 7.** Measure of false positive rate

## 7. CONCLUSION

By adapting the permanent girth clustering model, the process of identification of a multiple set of intrusion attacks is handled in WSN. Once the abnormality of the traffic pattern is identified, a set of clusters are built based on the occurrence of irregularities over the nodes in the network. The benefits of using PC clustering model for multiple intrusion attacking process is presented as detect ing abnormal traffic patterns, distinguish attacks that have not formerly been observed, reduces the energy consumption by detecting multiple attacks in WSN and achieve high detection accuracy with low false positive rate for a multiplicity of replicated routing attacks. Simulation evaluation is conducted with set of sensor nodes to estimate the performance of the proposed PC model for multiple intrusion detection attacks against sequential hypothesis testing. Evaluation results revealed that the PC model consumes less energy approximately 12% for identifying the intrusion routing attacks in WSN with low positive rates.

## 8. REFERENCES

Gupta, G.R. and N.B. Shroff, 2010. Delay analysis for wireless networks with single hop traffic and general interference constraints. IEEE/ACM Trans. Netw., 18: 393-405. DOI: 10.1109/TNET.2009.2032181

Ho, J.W., M. Wright and S.K. Das, 2009. Fast detection of replica node attacks in mobile sensor networks using sequential analysis. Proceedings of the IEEE Browse Conference Publications INFOCOM., Apr. 19-25, IEEE Xplore Press, Rio de Janeiro, pp: 1773-1781. DOI: 10.1109/INFCOM.2009.5062097

Kim, J., X. Lin, N.B. Shroff and P. Sinha, 2010. Minimizing delay and maximizing lifetime for wireless sensor networks with anycast. IEEE/ACM Trans. Netw., 18: 515-528. DOI: 10.1109/TNET.2009.2032294

La, R.J. and E. Seo, 2011. Expected routing overhead for location service in manets under flat geographic routing. IEEE Trans. Mobile Comput., 10: 434-448. DOI: 10.1109/TMC.2010.188

Li, G., J. He and Y. Fu, 2008. A group-based intrusion detection scheme in wireless sensor networks. Proceedings of the 3rd International Conference on Grid and Pervasive Computing Workshops, May. 25-28, IEEE Xplore Press, Kunming, pp: 286-291. DOI: 10.1109/GPC.WORKSHOPS.2008.31

Li, H., V. Pandit, N. Katneni and D.P. Agrawal, 2012. A reverse gaussian deployment strategy for intrusion detection in wireless sensor networks. Proceedings of the IEEE International Conference on Communications, Jun. 10-15, IEEE Xplore Press, Ottawa, DOI: 10.1109/ICC.2012.6364856

Misra, S, G. Xue and J. Tang, 2010. Constrained relay node placement in wireless sensor networks: Formulation and approximations. IEEE/ACM Trans. Netw., 18: 434-447. DOI: 10.1109/TNET.2009.2033273

Stavrou, E. and A. Pitsillides, 2011. Combating persistent adversaries in wireless sensor networks using directional antennas. Proceedings of the 18th International Conference on Telecommunications, May 8-11, IEEE Xplore Press, Ayia Napa, pp: 433-438. DOI: 10.1109/CTS.2011.5898964

Thamilarasu, G., A. Balasubramanian, S. Mishra and R. Sridhar, 2005. A cross-layer based intrusion detection approach for wireless ad hoc networks. Proceedings of the IEEE International Conference on Mobile Adhoc and Sensor Systems Conference, Nov. 7-7, IEEE Xplore Press, Washington, DC., 861- 861. DOI: 10.1109/MAHSS.2005.1542882

Xing, K., F. Liu, X. Cheng and D.H.C. Du, 2008b. Real-time detection of clone attacks in wireless sensor networks. Proceedings of the 28th International Conference Distributed Computing Systems, Jun.17-20, IEEE Xplore Press, Beijing, pp: 3-10. DOI: 10.1109/ICDCS.2008.55

Xing, K. and X. Cheng, 2010. From time domain to space domain: Detecting replica attacks in mobile ad hoc networks. Proceedings of the IEEE INFOCOM, Mar. 14-19, IEEE Xplore Press, San Diego, CA., pp: 1-9. DOI: 10.1109/INFCOM.2010.5461977

Xing, K., F. Liu, X. Cheng and D.H.C. Du, 2008a. Real-time detection of clone attacks in wireless sensor networks. Proceedings of the 28th International Conference on Distributed Computing Systems, Jun.17-20, IEEE Xplore Press, Beijing, pp: 3-10. DOI: 10.1109/ICDCS.2008.55

Yu, C.M., C.S. Lu and S.Y. Kuo, 2009. Efficient and distributed detection of node replication attacks in mobile sensor networks. Proceedings of the 70th Vehicular Technology Conference Fall, Sept. 20-23, IEEE Xplore Press, Anchorage, AK., pp: 1-5. DOI: 10.1109/VETECF.2009.5379092

Yu, Z. and G. Yong, 2010. A dynamic en-route filtering scheme for data reporting in wireless sensor networks. IEEE/ACM Trans. Netw., 18: 150-163. DOI: 10.1109/TNET.2009.2026901

Zhu, B., S. Setia, S. Jajodia, S. Roy and L. Wang, 2010. Localized multicast: Efficient and distributed replica detection in large-scale sensor networks. IEEE Trans. Mobile Comput., 9: 913-926. DOI: 10.1109/TMC.2010.40