IJESRT

INTERNATIONAL JOURNAL OF ENGINEERING SCIENCES & RESEARCH TECHNOLOGY

NODE CATEGORISATION ALGORITHMS IN WIRELESS SENSOR NETWORK: A COMPARATIVE STUDY

Ayushi Nainwal*, Arvind Kalia, Jawahar Thakur

[*] Department of Computer Science Himachal Pradesh University
Department of Computer Science Himachal Pradesh University
Department of Computer Science Himachal Pradesh University

DOI: 10.5281/zenodo.168436

ABSTRACT

Wireless sensor network are often installed in unattended environment for monitoring and sending information to base station. If nodes in the network are compromised then the security of the network degrades quickly. There have been many approaches researched to tackle this issue. This paper introduces three node categorisation algorithms named Global Ranking Algorithm, Stepwise Ranking Algorithm and Hybrid Ranking Algorithm, which can identify misbehaving forwarders that drop or modify packets. In network each packet is padded and encrypted so as to hide the source of the packet. The packet mark, a small number of extra bits, is added to each packet such that the sink node can recover the source of the packet and then figure out the dropping ratio associated with every sensor node. Finally, the node categorization algorithms can identify nodes that are packet droppers for sure, suspiciously packet droppers, not packet droppers based on dropping ratio. This paper analyses and compares the three ranking algorithms on the basis of detection rate and false positive probability. Extensive analysis is conducted by running each algorithm in java eclipse.

KEYWORDS: Global Ranking –Based (GR) Approach, Stepwise Ranking-Based (SR) Approach, Hybrid Ranking-Based (HR) Approach.

INTRODUCTION

The Wireless sensor network consists of sensing node and sink. The purpose of such node is to sense medium and gathers information and forwards that information to base station or central authority that controls all nodes in the network [13]. Because of the ease of deployment, the low cost of sensor nodes and the capability of self organization, a sensor network is often deployed in an unattended and hostile environment to perform the monitoring and data collection tasks [2]. When it is deployed in such an environment, it lacks physical protection and is subject to node compromise. After compromising one or multiple sensor nodes, an intruder may launch various attacks to disrupt the network communication. Among these attacks, two common ones are dropping packets and modifying packets, i.e., compromised nodes drop or modify the packets that they are supposed to forward [8]. To avoid these two kinds of attack we need to provide some method to identify these compromising nodes. This can be done by padding the encrypted packet with packet mark. The packet mark, a small number of extra bits, is added to each packet so that the sink node can recover the source of the packet and then figure out the dropping ratio associated with every sensor node. Finally, our node categorization algorithms can rank nodes as packet droppers for sure, suspiciously packet droppers, not packet droppers. Each node undergoes heuristic process in order to receive rank and thereby remove the malicious and compromised node in the network [10]. The following heuristics ranking algorithm are used to categorize nodes in the network: Global Ranking, Selective Ranking and Hybrid Ranking.

1. Global ranking based approach: The Global ranking method [5] is based on assumption that if a node is identified as suspiciously bad then there are more chances that the node is a bad node. The node with the highest value of accused account is chosen as a bad node for sure and all the pairs that contain this node are removed.

2. Stepwise ranking based approach: It may happen that the Global Ranking method falsely accuses innocent nodes that were parents or children of bad nodes [4]. So to remove this problem if a bad node u is found and there is a node v that is been suspected together with node u, the value of node v account is reduced by the times u and v have been suspected together.

3. Hybrid Ranking-Based (HR) Approach: The Global Ranking Method and the Selective Ranking method [12] detect bad nodes with some false accusations so Hybrid Ranking method is used. The Hybrid Ranking approach also considers accusation account value as Global Ranking and Selective Ranking but it checks if an innocent node is not being framed by previously identified bad nodes. In this method first all of the likely bad nodes are identified, and then the one with highest account value is chosen only if the node has not always been accused together with the bad nodes that were identified before.

In this paper we have evaluated and compared the three ranking algorithms. The performance is analyzed by means of detection rate and false positive probability. The rest of paper is organized as follows: Section 2 gives a brief review of all the concerned research papers. It provides a brief discussion of the other contributors and their conclusions. Section 3 discusses the main objectives of research. Section 4 describes the overview of implementation performed. Sections 5 give the results of the research and provide discussion about the same. Finally conclusion is given in the end summarizing the key points and other related considerations.

LITERATURE REVIEW

Chuang et al.**[1]** evaluate the effectiveness and efficiency of the packet dropper and modifier identification scheme using ns-2 simulator. They compared the node categorisation algorithm on the basis of two parameters the detection rate and the false positive probability, concluding that the hybrid ranking is the best algorithm. **Geri and Ozery[10]** review the node classification problem by using algorithms based on graph minimum cuts. They determined the node behaviour in both online and offline mode by looking at the neighbour node. **Jenifer and Dorai.D[6]** studied three ranking scheme named Universal ranking , Iterative ranking and Hybrid ranking for identifying pure nodes participating in communication network. They performed simulation on ns2 and effectively proved that both iterative and universal ranking algorithms perform poor compared to hybrid algorithm. **Ning et al.[9]** proposed new hybrid MAC protocol with three phases initialization phase, cluster formation phase and data propagation phase in order to classify nodes in wireless sensor network and provides maximal reliability, energy efficiency, and scalability. **Atakli et al.[5]** used the concept of weight-based network to detect malicious nodes. According to this if sensor node is compromised its weight is likely to be lower than a specific threshold, hence we can identify it as a malicious node.

OBJECTIVES

The objectives of this evaluation are
1) Evaluate the Global Ranking Algorithm, Stepwise Ranking Algorithm and Hybrid Ranking Algorithm on the basis of detection rate and false positive probability.
2) Compare the various node categorization algorithms and determine the most effective and efficient algorithm for node ranking.
In order to meet the objective quantitative approach [3] has been used. The best algorithm is determined by statistically analyzing the data obtained.

IMPLEMENTATION

In order to evaluate the effectiveness of the various algorithms an implementation is conducted in java. Algorithms are implemented as followed, each suspicious node has an accused account associated with it which keeps track of the number of time the node has been identify as bad nodes. To determine the most likely set of bad nodes after certain rounds of detection, following Algorithms are used.

Algorithm 1: The Global Ranking-Based Approach
Step 1. Sort all suspicious nodes into queue Q according to the descending order of their accused account values.
Step 2. The node u with the highest value is chosen as a most likely bad node. Remove node u from queue Q and add it to queue X consisting of bad nodes.
Step 3. Remove all the pairs that contain node u ,from queue Q.
Step 4. Repeat the process until all suspicious nodes have been removed.

Algorithm 2: The Stepwise Ranking-Based Approach
Step 1. Sort all suspicious nodes into queue Q according to the descending order of their accused account values.
Step 2. The node u with the highest value is chosen as a most likely bad node

Step 3. Once a bad node u is identified, for any other node v that has been suspected together with node u, the value of node v accused account is reduced by the times that u and v have been suspected together.
Step 4. Remove node u from queue Q and add it to queue X consisting of bad nodes.
Step 5. Repeat the process until all suspicious nodes have been removed.

Algorithm 3 The Hybrid Ranking-Based Approach
Step 1. Sort all suspicious nodes into queue Q according to the descending order of their accused account values.
Step 2. The node u with the highest value is chosen as a most likely bad node
Step 3. After a most likely bad node has been chosen, the one has the highest accused account value among the rest is chosen only if the node has not always been accused together with the bad nodes that have been identified already.
Step 4. Remove node u from queue Q and add it to queue X consisting of bad nodes.
Step 5. Repeat the process until all suspicious nodes have been removed.
The performance of the ranking algorithms is measured using two aspects: the detection rate[7], defined as the ratio of successfully identified bad nodes, and the false positive probability[11], defined as the ratio of mis-accused innocent nodes over all innocent nodes. JAVA project is created on Easy Eclipse Server Java 1.2.2.2 connected to mysql database.
The network topology is generated randomly with certain nodes declared as compromised nodes.
Compromised nodes might treat packets generated by themselves and those by other nodes differently.
For its own packets, a compromised node may
(1) Drop the packets at each round
(2) Drop the packets in some randomly rounds
(3) Do not drop all the time.
For other nodes' packets that it is supposed to forward, a compromised node may
(1) Drop the packets in each round
(2) Drop the packets in some randomly rounds.
Considering the combination of dropping behaviours in the above two categories, we obtain six attack models in total namely, attack models 1-1, 1-2, 2-1, 2-2, 3-1 and 3-2, where the first index represents the dropping behaviour towards the packets of the bad node itself and the second index represents the dropping behaviour towards others packets. Three node categorization algorithms namely, stepwise ranking (SR) algorithm, global ranking (GR) algorithm, hybrid ranking (HR) algorithm are applied on the specified attack models and are compared.

RESULTS AND ANALYSIS

The results have been arrived at keeping in view the detection rate and false positive probability of algorithms under different attack modes, the impact of the Number of Rounds on categorisation algorithms and the impact of Percentage of Bad Nodes on categorisation algorithm. Following result were obtained.

Global Ranking Algorithm
a) Evaluation of Global Ranking Algorithm The figure 5.1 to 5.12 shows the variation in detection rate and false positive probability of Global Ranking Algorithm under different attack models. From these figures we can see that the detection rate for Global Ranking Algorithm is around 0.65 when numbers of rounds are less whereas the detection rate increases as the number of rounds increases. Similarly the false positive probability is quite high when numbers of rounds are less, but it slowly tends to decrease with increase in number of rounds.
b) Impact of the Number of Rounds
The figures show that stable and high detection rate as well as low false positive probability is achieved when the numbers of rounds are high. The result reveals that after 8 rounds approximately all bad nodes are detected and also false positive probability decreases.
c) Impact of Percentage of Bad Nodes Generally the less the number of bad nodes the easier it is to detect them. Global Ranking Algorithm identifies bad nodes based on number of time they are suspected to be malicious nodes. So, as the number of bad nodes increases more rounds are needed to detect them.

Selective Ranking Algorithm
a) Evaluation of Selective Ranking Algorithm The figures show that Selective Ranking Algorithm is comparatively better than Global Ranking Algorithm in terms of detection rate and false positive probability. The amount of fluctuation in false positive probability is quite small compare to that of Global Ranking Algorithm. Hence it can be concluded that Selective Ranking is better than Global Ranking Algorithm.

b) Impact of the Number of Rounds The above evaluation clears that Selective Ranking Algorithm has high detection rate compare to Global Ranking, this means that it detects more bad nodes in few rounds. The lesser the number of rounds needed to detect bad nodes the more efficient is the algorithm.

c) Impact of Percentage of Bad Nodes Result shows that for Selective Ranking Algorithm as the number of bad nodes increases more rounds are needed to detect them. However the numbers of rounds needed are comparatively less than the rounds required by Global Ranking Algorithm.

Hybrid Ranking Algorithm

a) Evaluation of Selective Ranking Algorithm This Algorithm combines the advantages of both Selective Ranking Algorithm and Global Ranking Algorithm thereby show highest detection rate and lowest false positive probability. The fluctuation in false positive probability is quite small compare to both Selective Ranking Algorithm and Global Ranking Algorithm. This mean that Hybrid Ranking Algorithm detects bad nodes faster and hence is the best algorithm for node ranking in wireless sensor network.

b) Impact of the Number of Rounds The above evaluation clears that Hybrid Ranking Algorithm has high detection rate compare to Global Ranking, and Selective Ranking, this means that it detects more bad nodes in few rounds. The lesser the number of rounds needed to detect bad nodes the more efficient is the algorithm.

c) Impact of Percentage of Bad Nodes Result shows that for Hybrid Ranking Algorithm as the number of bad nodes increases more rounds are needed to detect them. However the numbers of rounds needed are comparatively less than the rounds required by Global Ranking Algorithm and Selective Ranking Algorithm.

1) Attack Model 1-1 The first attack model represents the node that drops its own packet at each round as well as drop all the packets forwarded by other nodes.

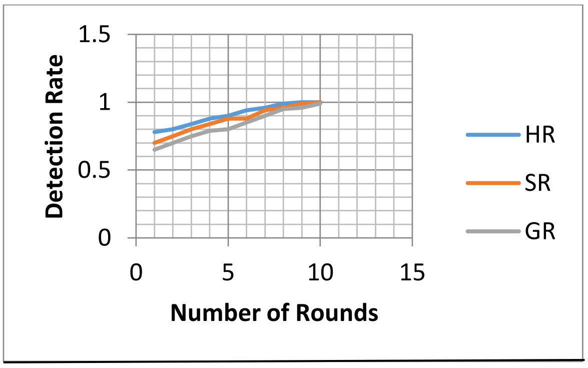

FIGURE 5.1 DETECTION RATE

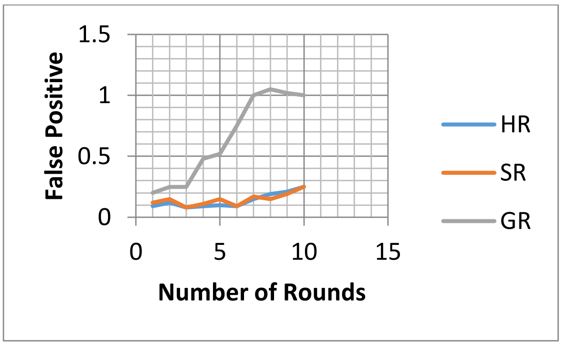

FIGURE 5.2 FALSE POSITIVE PROBABILITIES

2) ATTACK MODEL 1-2 The second attack model represents the node that drops its own packet at each round but drop the packets forwarded by other nodes in some randomly rounds.

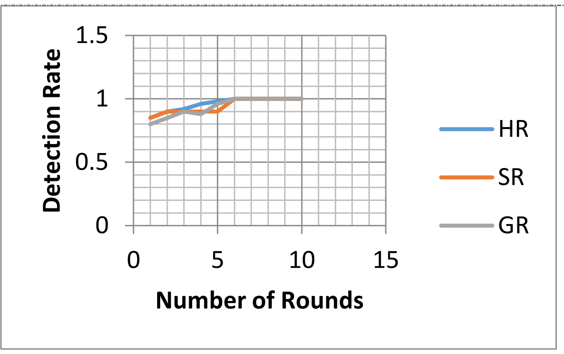

FIGURE 5.3 DETECTION RATE

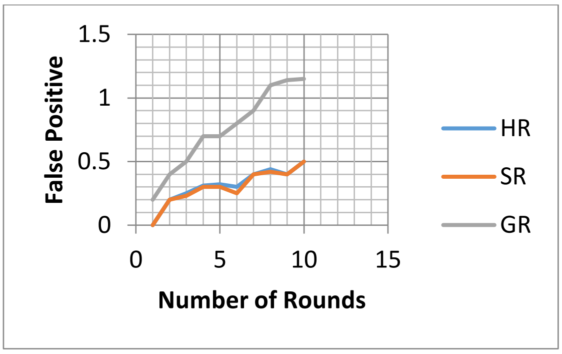

FIGURE 5.4 FALSE POSITIVE PROBABILITIES

3) ATTACK MODEL 2-1 The third attack model represents the node that drops its own packet in some randomly rounds but always drop the packets forwarded by other nodes.

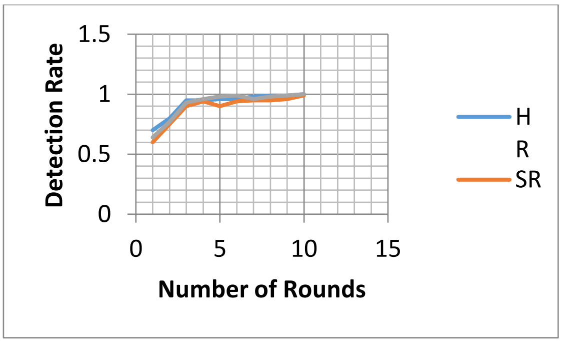

FIGURE 5.5 DETECTION RATE

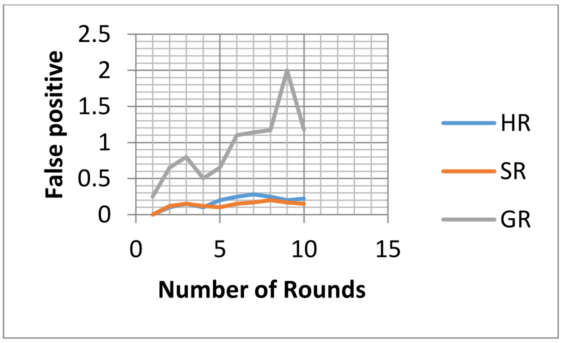

FIGURE 5.6 FALSE POSITIVE PROBABILITIES

ISSN: 2277-9655
Impact Factor: 4.116
CODEN: IJESS7

4) ATTACK MODEL 2-2 The fourth attack model represents the node that drops its own packet and the packets forwarded by other nodes in some randomly rounds.

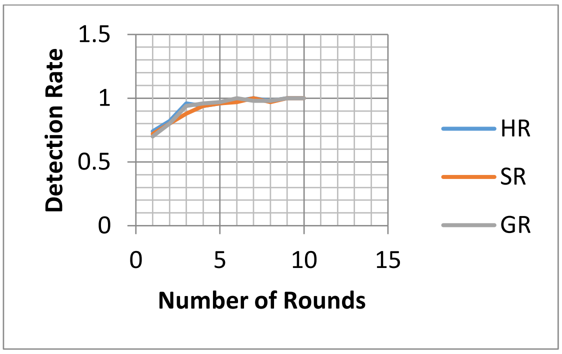

FIGURE 5.7 DETECTION RATE

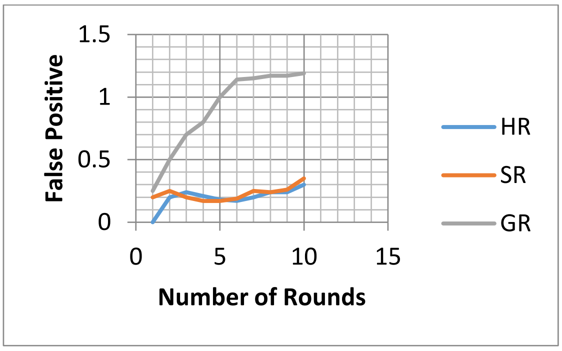

FIGURE 5.8 FALSE POSITIVE PROBABILITIES

5) ATTACK MODEL 3-1 The fifth attack model represents the node that never drops its own packet but always drop the packets forwarded by other nodes.

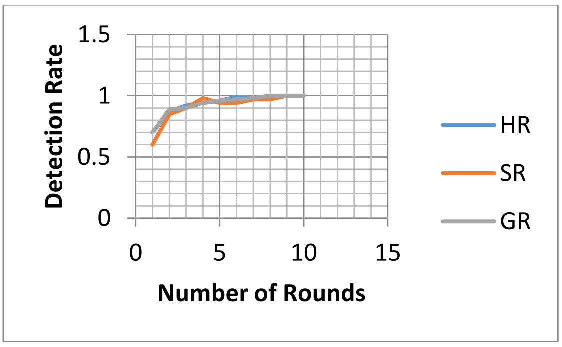

FIGURE 5.9 DETECTION RATE

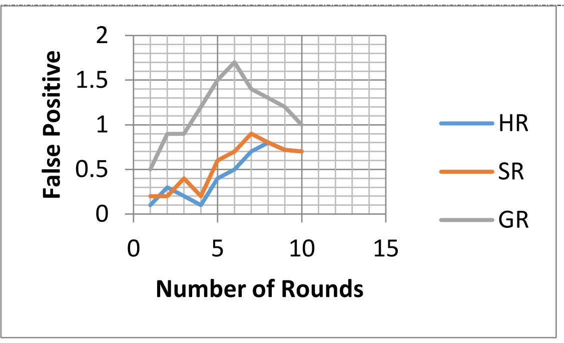

FIGURE 5.10 FALSE POSITIVE PROBABILITIES

6) ATTACK MODEL 3-2 The sixth attack model represents the node that never drops its own packet but drop the packets forwarded by other nodes in some randomly rounds.

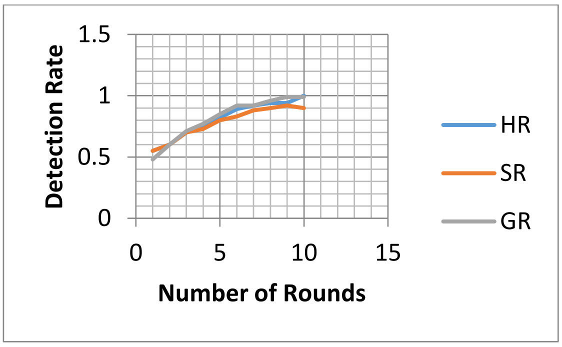

FIGURE 5.11 DETECTION RATE

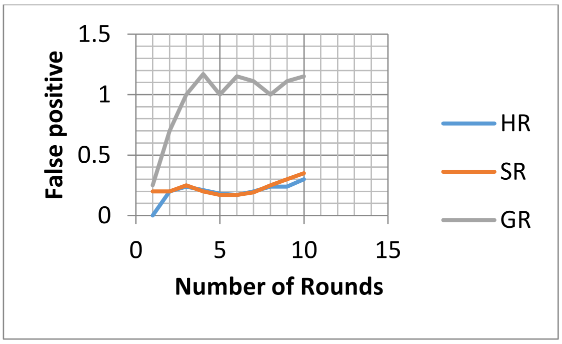

FIGURE 5.12 FALSE POSITIVE PROBABILITIES

CONCLUSION

This paper compares three ranking algorithms which are used to identify malicious nodes among all nodes participating in communication network. All three algorithms are compared on the basis of detection rate and false positive probability. Extensive analysis was conducted by running each algorithm in java eclipse. The results show that Hybrid Ranking Algorithm has highest detection rate and lowest false positive probability. Hence it is concluded that Hybrid Ranking Algorithm is most effective and efficient algorithm for node categorisation.

REFERENCES

[1] Chuang Wang, Taiming Feng , Jinsook Kim, ”Catching Packet Droppers and Modifiers in Wireless Sensor Networks”, IEEE Transactions on Parallel and Distributed Systems Volume: 23, Issue: 5, **Page(s):** 835 – 843,May 2012.

[2] C.Sahaya Kingsly, Dr. J. George Chellin Chandran, ”Critical Study on Constraints in Wireless Sensor Network Applications”, Vol.2 - Issue 7, July - 2013.

[3] D. Amogh," Identifying Misbehaving Nodes in Wireless Sensor Networks", International Journal of Engineerg Trends and Technology (IJETT) – Volume 24 Number 6- June 2015.

[4] Earl R., Babbie,*"The Practice of Social Research",* 12th ed. Belmont, CA: Wadsworth Cengage, 2010; London: SAGE Publications, 2010.

[5] Hemanth Kumar Chinta, Venkata Ramana K, "Novel Techniques to Counterfiet the Compromising Attacks In Wireless Sensor Network", International Journal of Innovative Research in Computer and Communication Engineering,Vol.3, Special Issue 6, August 2015.

[6] HE Williams, D.Lane," Web database applications with PHP and MySQL", 2004.

[7] Idris M. Atakli, Hongbing Hu and Yu Chen,"Malicious Node Detection in Wireless Sensor Networks using Weighted Trust Evaluation", Proceedings of the 2008 Spring simulation multiconference, Pages 836-843, 2008 .

[8] Ismail Butun , Salvatore D. Morgera , Ravi Sankar," A Survey of Intrusion Detection Systems in Wireless Sensor Network",IEEE Communications Surveys & Tutorials (Volume: 16, Issue: 1, First Quarter 2014)

[9] Jenifer.G and Ramya Dorai.D, "Evaluating pure nodes in wireless sensor networks", International journal of advanced technology in engineering and science, Volume no.02, Issue no. 05, May 2014.

[10] K Arnold, Gosling,,D. Holmes, The Java programming language, 2000 -etf.beastweb.org.

[11] Kenjiro Cho, Philippe Jacquet,**"**Technologies for Advanced Heterogeneous Networks" , 24-Nov 2005

[12] Mohamed-Lamine Messai," Classification of Attacks in Wireless Sensor Networks", International Congress on Telecommunication and Application, 23-24 APRIL 2014

[13] Ning Sun, Youngbuk Cho and Sangho Lee, "Node Classification Based on Functionality in Energy-Efficient and Reliable Wireless Sensor Networks", International Journal of Distributed Sensor Networks December 2012 Vol. 8 No. 12.

[14] Ofir Geri and Or Ozery," Node Classification in Wireless Sensor Network"IEEE Infocom 2006, April 2006.

[15] S. Swapna Kumar, "A Guide to Wireless Sensor Networks" 2013.

[16] S.VIJAYALAKSHMI,R.KURINJIMALAR, S.PRAKASH," Detection of Packet Dropping and Modification in Wireless Sensor Network"', International Journal of Computer Science & Engineering Technology (IJCSET), Vol. 4 No. 04 Apr 2013.

[17] V. Bhuse, A. Gupta, and L. Lilien,"Dpdsn: Detection of packet-dropping attacks for wireless sensor networks," In the Trusted Internet Workshop,International Conference on High Performance Computing, December 2005.

[18] Y Li, MT Thai," Wireless sensor networks and applications", 2008.

[19] Y Xue, HS Lee, M Yang, P Kumarawadu, " Performance evaluation of ns-2 simulator for wireless sensor networks", Electrical and Computer Engineering, 2007. CCECE 2007.