ISSN- 2350-0530(O) ISSN- 2394-3629(P)
IF: 4.321 (CosmosImpactFactor), 2.532 (I2OR)

INTERNATIONAL JOURNAL OF RESEARCH – GRANTHAALAYAH
A knowledge Repository

Science

# MODELING AND SIMULATION OF THRESHOLD ANALYSIS FOR PVFS IN WIRELESS SENSOR NETWORKS

**Tae Ho Cho [*1], Su Man Nam [2]**
[*1] College of Software, Sungkyunkwan University, KOREA
[2] College of Information and Communication Engineering, Sungkyunkwan University, KOREA

**DOI:** 10.5281/zenodo.60963

## ABSTRACT

***Wireless sensor networks (WSNs) suffer serious damage from false positive and negative attacks due to their hardware restrictions. The sensor network causes both unnecessary energy consumption and information loss through false reports and normal reports, which include false message authentication codes (MACs). A probabilistic voting-based filtering scheme (PVFS) effectively detects the two types of attacks through a pre-defined threshold, which is the number of detected false MACs in a report. Since the threshold significantly influences the ability to detect attacks, the sensor network should be simulated to ensure proper function. In this paper, we describe the development and simulation of a PVFS-based WSN using a discrete event system specification. The experimental results showed that PVFS with a threshold of 2 reduced energy usage by about 16% and improved the detected false reports as compared with a PVFS with a threshold of 3.***

**Keywords:**
*modeling and simulation; wireless sensor networks; probabilistic voting-based scheme; threshold analysis.*

**Cite This Article:** Tae Ho Cho, and Su Man Nam, "MODELING AND SIMULATION OF THRESHOLD ANALYSIS FOR PVFS IN WIRELESS SENSOR NETWORKS" International Journal of Research – Granthaalayah, Vol. 4, No. 8 (2016): 1-10.

## 1. INTRODUCTION

Wireless sensor networks (WSNs) are being applied in various fields. The WSN consists of a large number of sensor nodes and a base station [1-3]. The sensor nodes sense events and forward the event data, and the base station (BS) collects the data and notifies the users of the event information. Since the sensor network is operated in an open-collaborative and large-scale environment without an infrastructure, the nodes are susceptible to attacks from software and hardware threats. Moreover, adversaries can inject various attack patterns into the network. False positive [4, 5] and false negative attacks [5], which are generated in an application layer, use false data injection and can cause serious damage to the network.

ISSN- 2350-0530(O) ISSN- 2394-3629(P)
IF: 4.321 (CosmosImpactFactor), 2.532 (I2OR)

A probabilistic voting-based filtering scheme (PVFS) [5] detects false positive and false negative attacks using a threshold, which is the number of verified false message authentication codes (MACs) in a report. Even though this scheme provides energy savings and detection power against the attacks, it is difficult to accurately detect the attacks due to the threshold. For example, if a low threshold is defined, the detection of false positive attacks is higher than the false negative attacks; on the other hand, if a high threshold is defined, the detection of false negative attacks is high.

In this paper, we propose a conceptual model of a PVFS-based WSN using discrete event system specification (DEVS) [6-8] for the threshold analysis, and we simulated the model based on time and state change. The sensor network is suitable for implementing DEVS because both have a hierarchical and modular structure.

The rest of this paper is organized as follows. Section 2 introduces the background, and Section 3 presents the PVFS-based WSN model. Section 4 provides a performance evaluation of the proposed model using analysis and simulation. We draw conclusions at the end of this paper.

## 2. BACKGROUND

In this section, we present related background works.

### *2.1.FALSE POSITIVE AND NEGATIVE ATTACKS*

In false positive attacks, a compromised node injects false reports into the sensor network about a non-existent event. If the false report arrives in the base station via multiple hops, the network consumes additional energy in the intermediate nodes due to false alarms in the BS. As a result of this attack, the sensor network lifetime decreases and the network loses some of its functions. To reduce the attacks, false reports are filtered out while forwarding the report.

In false negative attacks, a compromised node generates a false MAC and forwards it to the cluster head (CH) after the compromised node receives normal event data from its CH. If the CH attaches a false MAC in a report, the report will be dropped in a verification node due to the MAC. As a result, the BS loses the report data and cannot provide necessary information to users. Thus, the report (including the false MAC) is continually forwarded when the false MAC is detected.

### *2.2.PROBABILISTIC VOTING-BASED FILTERING SCHEME*

In PVFS, the base station creates a global key pool ($n$ partitions × $m$ keys), and each node receives each key from the BS. A cluster consists of a CH and the multiple member node within a hop. The source CH probabilistically selects its verification nodes based on distance. The verification nodes acquire each key from the source.

When an event occurs, a source CH broadcasts the event data to its MBs. The MBs generates a MAC through the data and forward the MAC to the CH. After the source CH collects all the

ISSN- 2350-0530(O) ISSN- 2394-3629(P)
IF: 4.321 (CosmosImpactFactor), 2.532 (I2OR)

MACs, it generates a report including randomly selected MACs and forwards this report to the BS.

While the report is being transmitted, the selected verification nodes verify the MACs in the report through their keys as the report arrives in the nodes. If the report verification result is normal, the report is transmitted to the next node. Once again, the BS verifies all the MACs in the report through its global key pool.

For example, a compromised node can attach multiple false MACs in a report and forward a false report. When a verification node receives the false report, the node verifies the MAC through its key, and then it increases the number of verified false MACs. If the count has not reached the defined threshold yet, the verification node continually forwards the report against the false negative attack. However, if the count exceeds the threshold, the node immediately drops the report against the false positive attack.

### *2.3.DISCRETE EVENT SYSTEM SPECIFICATION*

The DEVS formalism developed by Zeigler is a hierarchical and modular discrete event model used to analyze systems. DEVS has the advantages of model reusability, expandability, and availability compared to other simulators (e.g., ns3 [9], OPNET [10] and etc.). DEVS defines two type of models: atomic models and coupled models.

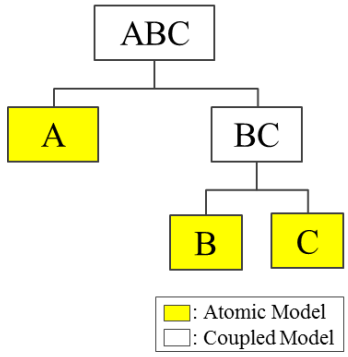


***Figure 1:*** DEVS models

Figure 1 shows a hierarchical structure with coupled models and atomic models. The coupled models are ABC and BC, and they include coupled models and atomic models. The atomic models are A, B, and C. The atomic models present dynamical behaviors of the system, and the coupled models indicate interactions between the atomic models.

#### *2.3.1. ATOMIC MODEL*

The atomic model is a basic model located in the bottom of the hierarchical structure that traces system operation. This model consists of three sets and four functions. The formalism of the atomic model M is as follows:

$M =< X, S, Y, \delta_{int}, \delta_{ext}, \lambda, ta >$
X: Set of external input event types

ISSN- 2350-0530(O) ISSN- 2394-3629(P)
IF: 4.321 (CosmosImpactFactor), 2.532 (I2OR)

S: Sequential state set
Y: Set of external vent types generated as output
$\delta_{int}$: Internal transition function
$\delta_{ext}$: External transition function
$\lambda$: Output function
$ta$: Time advance function

### *2.3.2. COUPLED MODEL*

The coupled model forms the combination atomic models or inferior coupled models. DEVS makes it possible to implement large and complex models due to these hierarchical characteristics [7]. The formalism of the coupled model DN is as follows:

$\mathrm{DN} =< \mathrm{D}, \{M_i\}, \{I_i\}, \{Z_{i,j}\}, select >$
D: Set of component names
$\{M_i\}$: Set of the basic model
$I_i$: Set of influences of I
$Z_{i,j}$: Output translation
$select$: Tie-breaking function

## 3. PVFS-BASED WSN MODEL DESING

We designed a PVFS-based WSN model and simulated the model to analyze the threshold required to effectively detect false positive and negative attacks.

### *3.1.MODEL DESIGN*

Figure 2 presents the structure of the PVFS-based WSN model. The model consists of a large number of coupled and atomic models. Every model forwards simulation content (e.g., event, packets) through its input and output ports. In the EF model, the GENR model randomly generates events, and the TRANSD model measures the PVFS-based WSN model processing results.

ISSN- 2350-0530(O) ISSN- 2394-3629(P)
IF: 4.321 (CosmosImpactFactor), 2.532 (I2OR)

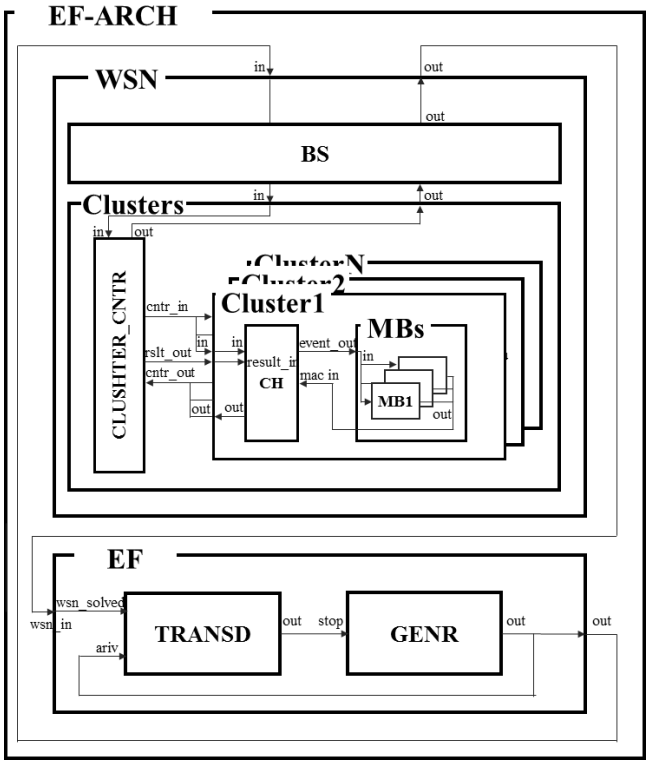


***Figure 2:*** Structure of the PVFS-based WSN model

### *3.2.MODEL DEFINITION*

In this section, major atomic models of the PVFS-based WSN model are discussed in detail.

A CH model is a DEVS model for a CH node of the sensor network. Figure 3 shows the CH state transition diagram.

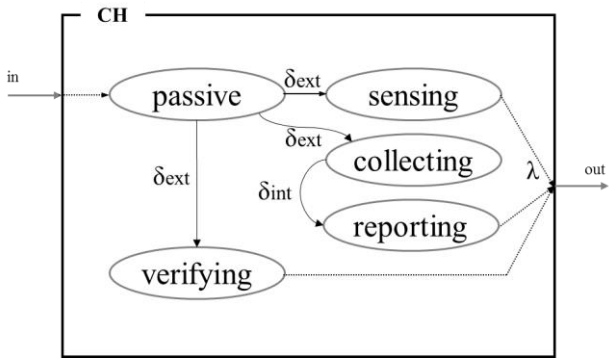


***Figure 3:*** State transition diagram of CH model

The CH model has five phases: *passive*, *sensing*, *collection*, *reporting*, and *verifying*. The model's initialization phase is *passive*. This model receives packets (event data, MACs, report) through the port *in* within the phase *passive* and transfers a phase among the next phases. After finishing execution of the model according to its phase, the model outputs a packet to transmit it to the next model.

ISSN- 2350-0530(O) ISSN- 2394-3629(P)
IF: 4.321 (CosmosImpactFactor), 2.532 (I2OR)

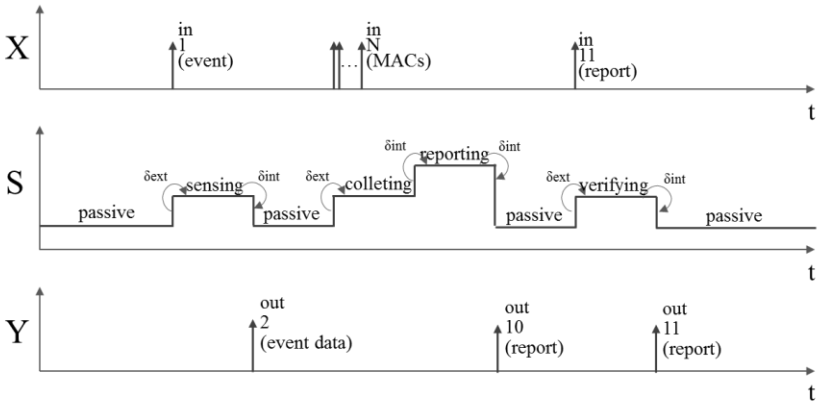


***Figure 4:*** Timing diagram of CH model

Figure 4 presents the timing diagram of the CH model. This model transfers *passive* to the next phase according to input (X) of three types. First, when the model receives an event, it transfers its states (S) and outputs (Y) event data through the port *out* to broadcast it to its MB models. Second, as it receives MACs, it outputs a report through the port *out* after executing phases *collecting* and *reporting*. Lastly, as a report arrives in the model, the model forwards the report through the phase *verifying*. Every packet is exchanged through its *id* between models.

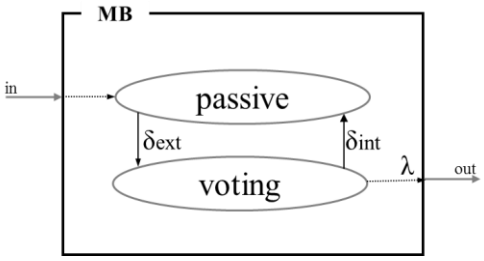


***Figure 5:*** State transition diagram of MB model

Figure 5 shows the state transition diagram of the MB model. The MB model has two phases, *passive* and *voting*, and the initialization phase is *passive*. After receiving event data through the port *in*, this model outputs a MAC through the port *out*.

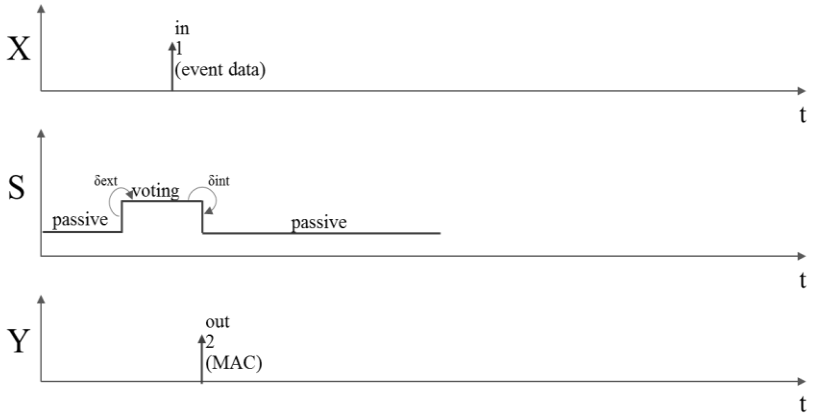


***Figure 6:*** Timing diagram of MB model

ISSN- 2350-0530(O) ISSN- 2394-3629(P)
IF: 4.321 (CosmosImpactFactor), 2.532 (I2OR)

Figure 6 shows the timing diagram of the MB model. When the model receives event data, it transfers *passive* to *voting*, and then this phase outputs the MAC.

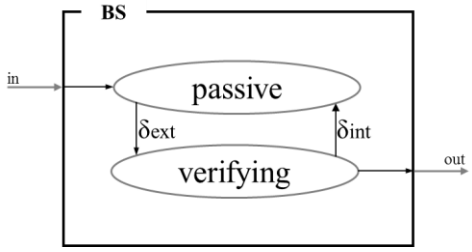


***Figure 7:*** State transition diagram of BS model

The state transition diagram of the BS model is as shown in Figure 7. The BS model has two phases: *passive* and *voting*. After the report arrives in this model through the port *in*, it transmits a verification result through the port *out*.

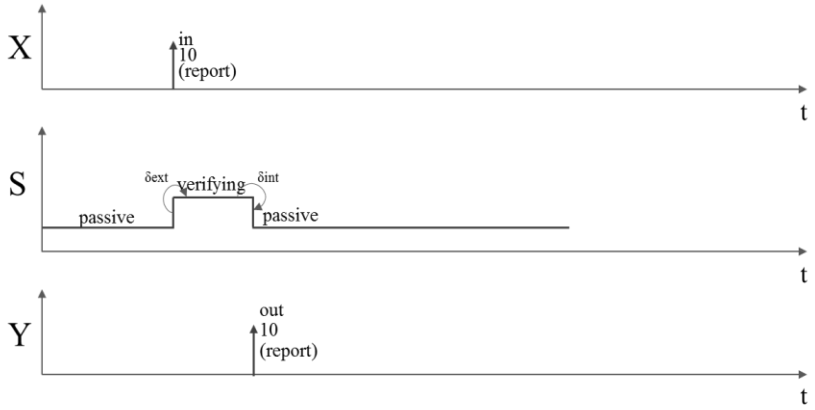


***Figure 8:*** Timing diagram of BS model

Figure 8 shows the timing diagram of the BS mode with two phases: *passive* and *verifying*. This model receives a report through the port *in*, and it outputs the result during the phase *verifying*.

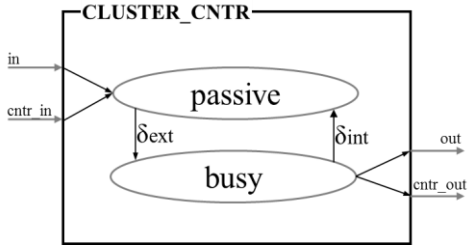


***Figure 9:*** State transition diagram of CLUSTER_CNTR model

Figure 9 shows the state transition diagram of the CLUSTER_CNTR model. This model includes *passive* and *busy*.

ISSN- 2350-0530(O) ISSN- 2394-3629(P)
IF: 4.321 (CosmosImpactFactor), 2.532 (I2OR)

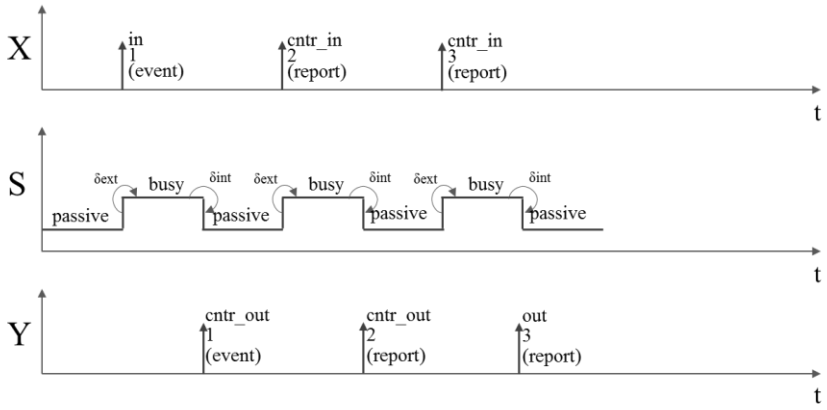


***Figure 10:*** Timing diagram of CLUSTER_CNTR model

Figure 10 shows the timing diagram of the CLUSTER_CNTR model. When this model receives an event generated from the GENR model, it selects the CH of a source cluster through the port *cntr_in*. When the report is received, the model forwards the report to the next CH model. If the report, which is en-route to the BS, arrives in the model, the report is transmitted through the port *out* during the phase *busy*.

## 4. SIMULATION RESULT

A simulation was performed to evaluate the PVFS with a threshold of 2 and a threshold of 3 using DEVS. The sensor field has a BS location in the lower-middle of the sensor field and contains 1,000 sensor nodes (100 CHs, 900 members). The size of the simulation environment was 1,000 X 1,000 $m^2$. The initial energies of CH and MB were 2 J and 1 J, respectively. Each node consumes 16.25 µJ per byte to transmit, 12.5 µJ per byte to receive, and 15 µJ per byte to generate packets [4]. Moreover, verification nodes consumed 75 µJ to verify the MAC. In this simulation, 300 events were randomly generated in the sensor field. The environment was set such that 10 nodes were compromised for false positive and negative attacks.

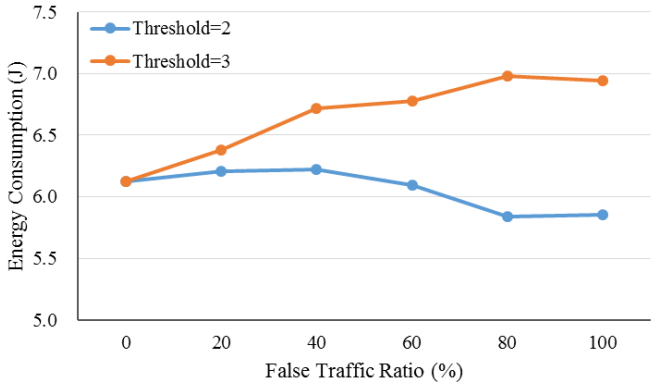


***Figure 11:*** False traffic ratio versus energy consumption

Figure 11 shows the false traffic ratio versus energy consumption of the sensor network. When FTR was 0%, the energy consumptions of threshold values of 2 and 3 were the same. When the false traffic increased, the gap in the energy consumption increased due to the generation of false

ISSN- 2350-0530(O) ISSN- 2394-3629(P)
IF: 4.321 (CosmosImpactFactor), 2.532 (I2OR)

positives and negative attacks. The PVFS with a threshold of 2 allowed for early detection of the false reports compared with a threshold of 3.

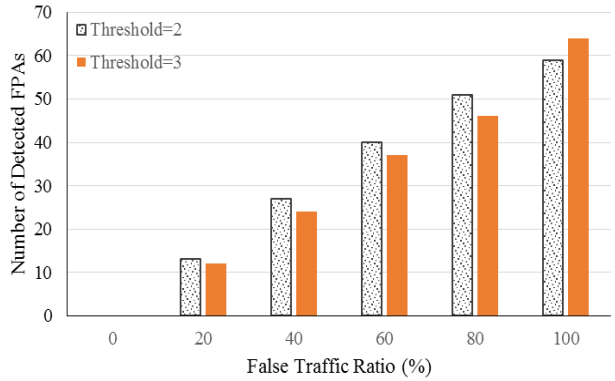


***Figure 12:*** False traffic ratio versus number of detected FPAs

Figure 12 shows the false traffic ratio versus the number of detected false positive attacks (FPAs). When the PVFS has a threshold of 2, the number of detected false reports increased as compared with a threshold of 3. Thus, many false reports were detected for a low threshold as compared to a large threshold.

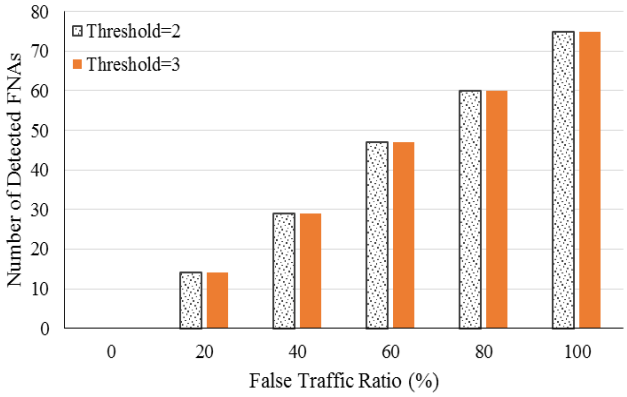


***Figure 13:*** False traffic ratio versus number of detected FNAs

Figure 13 shows the false traffic ratio versus the number of detected false negative attacks (FNAs). The number of detected FNAs is almost the same for both threshold values. Thus, changing the threshold may not influence the number of detected FNAs.

## 5. CONCLUSION

A sensor network can experience extensive damage such as energy and information loss from false positive and negative attacks due to node hardware restrictions. PVFS effectively detected these two types of attacks based on the number of detected false MACs in a report. In this paper, we designed a PVFS-based WSN model using a DEVS formalism and we simulated the performance of the sensor network to determine the effect of the threshold value. As shown in the simulation results, a PVFS with a threshold of 2 allowed the sensor network to save energy relative to a threshold of 3.

ISSN- 2350-0530(O) ISSN- 2394-3629(P)
IF: 4.321 (CosmosImpactFactor), 2.532 (I2OR)

## 6. ACKNOWLEDGMENTS

This research was supported by Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Education, Science and Technology (No. NRF-2015R1D1A1A01059484)

## 7. *REFERENCES*

*[1] X. Liu, "A Survey on Clustering Routing Protocols in Wireless Sensor Networks," Sensors, vol. 12, pp. 11113-11153, Aug., 2012.*

*[2] Weilian Su, Y. Sankarasubramaniam and E. Cayirci, "A survey on sensor networks," Communications Magazine, IEEE, vol. 40, pp. 102, 2002.*

*[3] R. V. Kulkarni, A. Forster and G. K. Venayagamoorthy, "Computational Intelligence in Wireless Sensor Networks: A Survey," Communications Surveys & Tutorials, IEEE, vol. 13, pp. 68-96, 2011.*

*[4] F. Ye, H. Luo, S. Lu and L. Zhang, "Statistical en-route filtering of injected false data in sensor networks," Selected Areas in Communications, IEEE Journal On, vol. 23, pp. 839-850, 2005.*

*[5] F. Li, A. Srinivasan and J. Wu, "PVFS: A Probabilistic Voting-based Filtering Scheme in Wireless Sensor Networks," International Journal of Security and Network, vol. 3, pp. 173-182, 2008.*

*[6] B. P. Zeigler, "DEVS theory of quantized systems," Advanced Simulation Technology Thrust DARPA Contract, 1998.*

*[7] B. P. Zeigler and H. S. Sarjoughian, "Introduction to devs modeling and simulation with java: Developing component-based simulation models," Technical Document, University of Arizona, 2003.*

*[8] B. P. Zeigler, Object-Oriented Simulation with Hierarchical, Modular Models: Intelligent Agents and Endomorphic Systems. Academic press, 1990.*

*[9] The ns-3 network simulator. Available: http://www.nsnam.org/.*

*[10] OPNET, "http://www.opnet.com/".*