Trusted-CDS Based Intrusion Detection System in Wireless Sensor Network (TC-IDS)

Amin Mohajer, Mohammad Hasan Hajimobini, Abbas Mirzaei, Ehsan Noori

High Speed Networking Lab (HSNL), Computer and Information Technology Engineering Department, Amirkabir University of Technology (Tehran Polytechnic), Tehran, Iran
Email: itgroup.hsnl@aut.ac.ir

Received 1 August 2014; revised 16 September 2014; revised 19 October 2014

Abstract

Security mechanism is a fundamental requirement of wireless networks in general and Wireless Sensor Networks (WSN) in particular. The Intrusion Detection System (IDS) has become a critical component of wireless sensor networks security strategy. There are several architectures for embedding IDS in WSN. Due to Energy Limitation, in this paper we use a distributed architecture which activates intrusion detection system for limited number of nodes. For this purpose we select a secure set of nodes called secure Connected Dominating Set (CDS). In this paper first, we propose a heuristic for selecting CDS based on weighing factor which uses the trust value. Trust is based on reputation and reputation refers to the opinion of one node about another node. Hence only well behaving and good quality nodes are selected as a dominant node for CDS construction. Then we activate IDS on these selected node set. In our proposed work the task of all dominating nodes is to discover any attack and threat that can affect the normal behavior of sensor nodes by analyzing actual status of a node, packet sent and received by node and measurement made to the environment. The simulation results show that our TC-IDS model have high packet delivery ratio, high throughput and low delay than existing IDS Schemes such as Lightweight IDS.

Keywords

Secure CDS, Wireless Sensor Network, Trust, Intrusion Detection System

Subject Areas: **Computer and Network Security, Cooperative Communications, Information and Communication: Security, Privacy, and Trust**

1. Introduction

A wireless sensor network is a network of simple sensing devices [1], which are capable of sensing some changes of incidents parameters and communicating with other devices, over a specific geographic area for some specific purposes like target tracking, surveillance, environmental monitoring etc. [2]. Since sensor nodes

How to cite this paper: Mohajer, A., Hajimobini, M.H., Mirzaei, A. and Noori, E. (2014) Trusted-CDS Based Intrusion Detection System in Wireless Sensor Network (TC-IDS). *Open Access Library Journal*, **1**: e848.
http://dx.doi.org/10.4236/oalib.1100848

are tightly constrained in processing ability, storage capacity and energy, routing and data aggregation in WSN are very challenging due to inherent characteristics. Therefore, sensor network needs to become autonomous and exhibit responsiveness and adaptability to evolution changes in real time, without explicit user or administrator action. This need is even more imperative when it comes to security threats, so an attempt to apply the idea of implementation of an IDS that can detect a third party attempts of exploiting possible insecurities and warn for malicious attack in WSN makes a lot of sense.

In case of wireless sensor network, the communication among the sensors is done using wireless transceivers. The threats that damaged the security in WSN can be detected by the Intrusion detection systems (IDSs). An IDS attempts to identify computer system, network intrusions and misuse by gathering and analyzing data. The wireless IDS can monitor and analyze user and system activities, recognize patterns of known attacks, identify abnormal network activity, and detect policy violations for WSN. Thus it is desirable to have several sensors that monitor the attacks and let each sensor report to a base station to avoid losing an important event [3]. In this paper, we explore the related issues for IDS in wireless sensor networks and a model for the implementation of IDS using concept of virtual backbone created by connected dominating set of sensor nodes.

According to energy limitations in WSNs, it is necessary to use architectures in which IDS is not active on all nodes. In this paper, for this purpose a method is proposed with 2 stages. In the first step, CDS nodes are selected based on a trust weighting factor. In the second step we activate IDS on the selected nodes. These intrusion detection systems detect the existing intrusions in the network through a cooperative process.

This paper is organized as follows. Section II describes related works associated with CDS construction and IDS issues. In section III, we present a trust-based method for CDS construction. In section IV we describe architecture of our IDS. Finally, after presenting the numerical results in section V, we concluded this paper in section VI.

2. Related Works

2.1. Connected Dominating Set: Issues

The nodes in a wireless sensor network are categorized into dominant nodes (CDS nodes) and dominate nodes. The connected structure of the dominant nodes creates a virtual backbone or a Connected Dominating Set (CDS). The adjacent nodes of dominant nodes are called dominate nodes. The messages transmitted by using this virtual backbone effectively reduce the communication overhead. The selection strategy of dominant node for connected dominating set construction is different for different approaches.

J. Wu and H. Li [4] proposed a simple and efficient algorithm for calculating the connected dominating set in a connected graph, which represents the scenario for a wireless network. In this paper they proposed a marking process that marks every vertex in a connected and un-weighted graph. A node is marked as dominant if two of its neighbors are not directly connected. To reduce the size of a connected dominating set, they proposed two rules.

RULE 1: If *u* and *v* are two vertices in a graph G, and $id(u) < id(v)$, then a marked node "*u*" can unmark itself if the marked node "*v*" covers it.

RULE 2: A marked node can unmark it, if it is covered by two other directly connected marked neighbors.

In **Figure 1(a)**, since $N(v) \quad N(u)$ and $\{id(v) < id(u)\}$, then the node *v* can unmark itself. In **Figure 1(b)**, the node *v* can unmark itself because of $N(v) N(u) N(w)$ and $id(v) = \min\{id(v), id(u), id(w)\}$. Wu and Li's approach performs well for finding a small dominating set than any other classical approaches. Each node gets its neighborhood information and their status (mark or unmark) by exchanging Hello messages. So it imposes communication overhead and high energy consumption. The main advantage of connected dominating set is that the routing information is localized to adapt the topological changes.

Another method for CDS framework is based on clustering. In the cluster-based category, the nodes are grouped into a set of clusters [5]. Generally in each cluster, a specific node called leader or Cluster-Head (CH) is designed to organize the set of specific functionalities within its cluster. The clusters are identified by the identity of the Cluster-Head. If the Cluster-Head fails, then the cluster no longer exists. A gateway node is one with at least two Cluster-Head as neighbors. The gateway node acts as a boundary node for each cluster. All other nodes belonging to a cluster are called Ordinary nodes. **Figure 2** depicts a cluster framework which consists of Cluster-Head, gateway and ordinary nodes. Cluster-Head schedules transmission and allocates resources within its cluster.

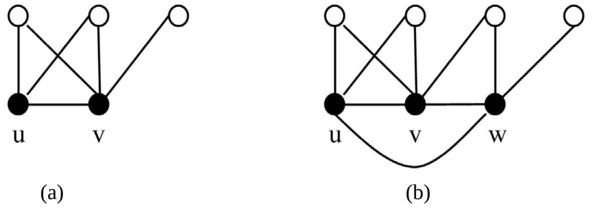

Figure 1. Two samples.

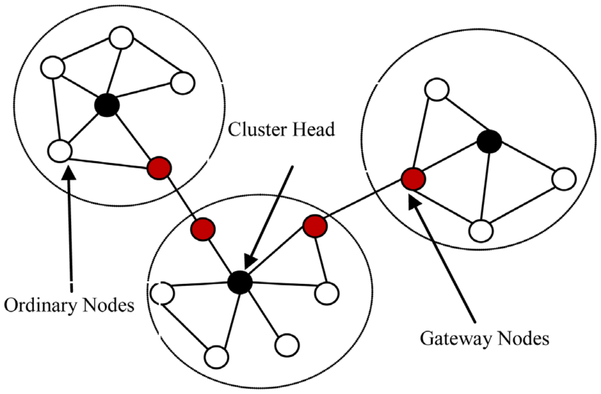

Figure 2. Clustering.

F. Theoleyre and F. Valois [6] proposed a virtual structure which consists of three phases: Neighborhood Discovery, Cluster formation, Backbone creation. Neighborhood discovery is performed by sending HELLO messages.

The cluster formation and Cluster-Head election is done by a distributed election and forms a cluster of radius Kcluster. A node moving inside a cluster does not make any topology changes. The Cluster-Heads and gateway nodes together form a CDS structure. The distance from a node to the backbone is at most kcds hops. A backbone helps to collect control traffic and to reduce overhead of route discovery. The integration of stable cluster formation and backbone creation creates an infrastructure that adapts to topological changes.

Ali Kies *et al.* [7] present a self organization framework based on weight parameter. Here the distance between the dominant node and dominate node is one hop. It is to limit the disconnection in the network. The weight parameter depends on quality of link, energy and connectivity. Equation (1) depicts the weight parameter.

$$\text{Pselection} = \alpha \times D + \beta \times E + \gamma \times M \tag{1}$$

where:

D: is the degree of the node;

E: represents the remaining energy level;

M: is the received signal strength;

α, β and γ: are the weighting factor.

To build the connected dominating structure, it acquires neighborhood knowledge by using the HELLO messages. In this approach, the dominant nodes have high energy, strong neighborhood and good quality of signal. This will help to avoid the frequent disconnection. But the problem with CDS construction is that the choice of misbehaving node as the dominant node will affect the network performance. Also, a distributed intelligent agent-based system is.

2.2. Intrusion Detection System: Issues

During the last few years, some works have been published where intrusion detection systems were applied in WSN environments [6]. Most of these studies have covered the local detection problem, where nodes detect specific attacks that happen in their network.

A description of the requirements of a WSN oriented IDS is given in [7]. Embedded systems, by definition, must use the minimum resources possible to preserve their lifetime. One of the main characteristic is that it must work with only localized and partial data due to the possible lack of centralized points with a global view. Other characteristics are that the system can never trust any node completely and that the system should be fully distributed. Finally, it should be able to withstand an attack to the IDS itself. A distributed intelligent agent-based system is proposed in [8]. It detects intrusions in a fully distributed way [9] [10]. This characteristic comes from the fact that all nodes have an independent IDS agent installed [11]. This agent is able to detect intrusions locally, always based on data collected by the same node and by neighbour nodes. Once an intrusion is detected, the responses or actions taken to isolate it are based on determines that is made collaboratively by the set of participating nodes. Other collaborative approaches on the local detection of selective forwarding and sinkhole attacks can be found in [12] and [13].

Regarding distributed systems, LIDeA is a Lightweight WSN oriented IDS [14]. It is based on a distributed architecture [15], where nodes listen to their neighbour nodes and collaborate with each other in order to detect an intrusion successfully.

3. Proposed CDS Model: Trusted CDS

The proposed CDS model is based on a weighing CDS factor which uses the trust value. The weighting factor depends upon energy, degree, willingness and trust factor of each node. This helps to reduce energy consumption, and thereby increasing the survivability of the network. Also this approach reduces the number of dropped packets.

3.1. Reputation

Reputation is the opinion of a node about another node. Reputation based frameworks helps to analyze the behavior of a node, *i.e*. whether the node is misbehaving or well-behaving by analyzing the previous history of a node.

3.2. Trust Factor Estimation

As every node of sensor network must store information about its surroundings in order to work properly. This information can be divided into two categories: knowledge about the security (an alert data base that contain information about alerts and suspicious nodes), and the knowledge about the environment (a list of the neighbors of the immediate neighbors of the node, which can be updated over the lifetime of the node using received messages). To determine the behaviour of a node, reputation and trust is used. If node A suspects about the confidence of node B, node A can ask the other nodes their reputation value for node B. The most shared opinion about the confidence of node B can confirm or discard the suspicions of node A. To determine the reputation of node B, node A takes into account the communications and iterations between them [14]. To calculate the reputation is used Beta distribution [16] [17] which uses correct and incorrect iterations to give a reputation value.

$$R_{ij} = \beta\left(\alpha_j + 1, \beta_j + 1\right) \tag{2}$$

where R_{ij} represents the confidence of the node *i* for node *j*, α_j are the cooperative iterations and β_j are the no cooperatives ones.

$$T_{ij} = E\left(\beta\left\{\alpha_i + 1, \beta_j + 1\right\}\right) = \frac{\alpha_i + 1}{\alpha_i + \beta_j + 2} \tag{3}$$

where T_{ij} is the trust of a node for other node, is given by a value from 0 to 1 (1 meaning absolute trust) and is based on Beta distribution.

On the other hand, if a node has doubts about another node and cannot determine with certainty if it is malicious or not because of lack of data, this node can ask its neighbourhood for information to determine with accuracy the aim of the suspicious node. The neighbourhood of a node is compounded by the nodes that are not farther than two hops. To calculate the new reputation of a node using the information given by the nodes in the neighbourhood, the same system of second hand information used in [18] and explained in [19] is applied.

$$\alpha_j^{NEW} = \alpha_j + \frac{\left\{2 \times \alpha_k \times \alpha_j^k\right\}}{\left\{(\beta_k + 2) \times \left(\alpha_j^k + \beta_j^k + 2\right)\right\} + \left\{2 \times \alpha_k\right\}} \tag{4}$$

$$\beta_j^{NEW} = \beta_j + \frac{\left\{2 \times \alpha_k \times \beta_j^k\right\}}{\left\{(\beta_k + 2) \times \left(\alpha_j^k + \beta_j^k + 2\right)\right\} + \left\{2 \times \alpha_k\right\}} \tag{5}$$

When a node asks for information about another node to the neighbourhood, it receives observations that nodes of neighbourhood have about the node in question $\left(\alpha_j^k, \beta_j^k\right)$, where α_j^k is the correct iterations performed by node *k* with node *j* and β_j^k are the incorrect ones.

With this second hand information a node can calculate the new iteration values that are used to recalculate the reputation. Moreover, information received from nodes with high reputation will have greater weight than those with less reputation.

3.3. Weighting Factor Estimation

The weight parameter depends on degree, energy, quality of the link, and trust value. Equation 6 depicts the weight parameter.

$$WF = D + E + WL + T \tag{6}$$

where:

- *WF*: is the weighting factor;
- *D*: is the degree of the node;
- *E*: represents the remaining energy level;
- *WL*: is the willingness of a node to become CDS;
- *T*: is the trust factor.

3.4. Heuristic for CDS Selection

The purpose of this CDS selection algorithm is to identify well behaving nodes as CDS and thereby optimizing the control overhead. In our reputation based system, there are two phases: Well-behaving node discovery based on the reputation value of and CDS construction based on the weight factor. In this section we describe about proposed heuristics for CDS selection based on a weight factor and reputation value. The proposed CDS heuristic is applied to each node *x* in network G as shown in **Figure 3**, the following terminologies will be used in describing the algorithm.

In this algorithm, CDS selector selects the well behaving node as dominant node. In step 2, it identifies the nodes that have connectivity from N1 to N2. This helps to avoid the unnecessary calculation of non-reachable nodes. Then it calculates the reputation value of all nodes which belonging to $R(x)$. Nodes can have a trust factor greater than 0.8 are added to the set $T(x)$. Calculate the weighing factor of every neighboring node which belongs to the set $T(x)$. In step 3, CDS selector selects the node having highest weighing factor as dominant node. If there is any tie (two or more nodes with the same value of weighing factor), a node with maximum remaining energy will be chosen. In addition if there is another tie, node which provide highest degree value will be selected as CDS node.

4. Architecture of the IDS

After selecting the trusted CDS, we activate the IDS on these nodes. In hierarchical IDS system, if an anomaly is detected a cooperated mechanism is initiated in order to take the decision of intrusion detection action while in our approach we used independent decision making system *i.e.* there are a no. of dominators node that have the task to perform the decision making functionality. They collect intrusion and anomalous activity evidences from other nodes and they make decision about network level intrusion. For an example if a node detects attack against the physical or logical safety *i.e.* they are being manipulated or not, must report to its any of dominator by raise an alarm, and this will take decision of intrusion by reporting to base station.

T_x	A set of neighbors of node ‘x’ which can have the trust value greater than 0.8
R(x)	Set of reachable nodes from N1 to N2
CDS(x)	CDS of node ‘x’.
N1	A set of 1 hop neighbors.
D(x)	A degree set of 1 hop neighbor of node ‘x’.
E(x)	Energy set of 1 hop neighbor of node ‘x’.
WF(x)	The weight factor of 1 hop neighbor of node ‘x’ $WF(x) = D_i + E_i + WL_i + T_i$
D_i	Degree of a node i (i is a member of N1)
E_i	Energy of a node i (i is a member of N1)
WL_i	Willingness of a node i (i is a member of N1)
T_x	The trust of a node x

```
Heuristic CDS(G=(V,E); N1; N2; R(x); T(x)⊂ V; CDS(x) ⊂ V )
Step 1    Initially, set CDS(x) = {}, R(x) = {} and T(x) = {}.
Step 2    For each node in N1, calculate the reachability.i.e. nodes in N2 which are reachable through N1. Add those nodes in the set R(x)
Step 3    While there exist nodes in R(x) :
    Step 3.1    For each node in R(x), calculate the reputation factor R(x) and add node with trust value greater than 0.8 to T(x).
    Step 3.2    For all nodes in T(x), calculate D(x), E(x),WL(x) ∀y ∈ T(x), where D(x) is the degree of the node, E(x) is the energy of the node and WL(x) is the willingness of the node to become a CDS.
    Step 3.3    Calculate the weight WF(x), where $WF(x) = D_i + E_i + WL_i + T_i$
    Step 3.4    Add node in T(x) that provide the highest weighted WF(x) to CDS(x)
    Step 3.5    If a tie case occurs in above step then Add node with maximum energy E(x) to the CDS (x).
    Step 3.6    If a tie case occurs in above step then Add node with maximum degree D(x) to CDS(x).
Step 4    Stop
```

Figure 3. Heuristic for CDS selection process.

As sensor nodes can operate on their own, however for propagating information on misbehaving nodes a platform to enable collaboration for dissemination of such IDS data is needed [20] [21]. The scope of a trusted dominating set based IDS deployed on a dense sensor are a helpful in selection of nodes to monitor and increase the scalability and detection accuracy of the IDS. It will be highly fault tolerant as well as enhances the security by providing maximum are a coverage using virtual backbone concept.

5. Simulation Results

We conducted simulations using NS2 [22], to determine the effectiveness of our proposed scheme and compare it with the Lightweight IDS approach in [23]. **Table 1** gives the simulation parameters.

To evaluate the performance of our scheme, we focused on three performance parameters: average throughput, packet delivery ratio and average end-to-end delay by considering nodes density and the number of traffic connection. For each scenario we performed ten random simulations. The performance metrics are described as follows:

- Average throughput: the amount of data that are delivered per second over the network;
- Packet delivery ratio (PDR): the ratio of total number of packets received by destinations to total number of packets sent by sources;
- Average end-to-end delay: the average amount of time for all packets to reach destination.

Table 1. Simulation parameters.

Parameter	Value
Number of Nodes	50 - 100
Simulation Time	500 s
Simulation Area	670 × 670 m^2
MAC	IEEE 802.11b
Initial Energy	1000 Joules
Transmission Power	1.4 W
Reception Power	1.2 W
Idle Power	0.9 W
Traffic Type	CBR
Packet Size	512 Bytes

Figure 4 shows that, false detection our scheme is better than Lightweight IDS. The low probability of false detection of TC-IDS is due to using trust along with IDS for detecting malicious nodes.

In our architecture, malicious nodes are detected by considering the trust in IDS that it helps to improve the security of the network.

PDRs of the two schemes are demonstrated in **Figure 5**. Trusted-proactive CDS based IDS has the highest PDR than Lightweight IDS, because stable and better nodes are selected as CDS nodes, based on a weighing factor which uses the trust value.

This avoids misbehaving nodes and these safe nodes perform the routing task in the network. Thus results in a higher packet delivery ratio. Detection rate of each architecture is highlighted in **Figure 6**. The detection rate of Lightweight IDS is lesser than TC-IDS.

In TC-IDS the intrusion detection is performed by CDS nodes which are selected using trust weighting factor. Also it uses intrusion detection rules along with trust in IDS detecting the malicious nodes. It results that the detection rate of proposed method gets close to 1, despite the growth of malicious nodes.

Figure 7 shows that PDR of Lightweight IDS decreases with increasing node density because in TC-IDS the packet routing task is done by trusted-CDS nodes. Hence dropping of packet is less in TC-IDS compared to Lightweight IDS. **Figure 8** shows delay with the number of nodes. According to **Figure 8**, TC-IDS have lower delay than Lightweight IDS as there will not be any broken links between the CDS nodes.

Figure 9 compares the PDR of architectures by varying the number of traffic connections. The PDR of TC-IDS is much better than Lightweight IDS. It is above 95%, while Lightweight IDS provide only 88%. The increase in the rate of traffic connection will not inversely affect the delivery of packets in TC-IDS. In **Figure 10**, the average throughput of TC-IDS is greater than that of Lightweight IDS because it limits the dropping of packet by introducing trusted CDS.

6. Conclusions

In this paper, we proposed a new CDS model for wireless sensor networks based on a weighing CDS factor which uses the trust value. The weighting factor also depends upon the energy, willingness and degree of a sensor node. The CDS heuristic helps to identify the best and well behaving nodes for the construction of CDS because the selfish dominant node will inversely affect the network performance. Here the nodes having highest weight factor and trust value are selected as CDS node. Then we activate the IDS on trusted-CDS nodes. An IDS further defenses the strength of a wireless sensor networks. In this paper we used an efficient scheme for IDS implementation which is more secure, provide efficient coverage and connectivity and minimize routing overheads. Also this helps to increase the survivability of the network.

The simulation results show that our model have high packet delivery ratio, high throughput and low delay than existing IDS scheme such as Lightweight IDS. In the future we test our proposed model with real experi-

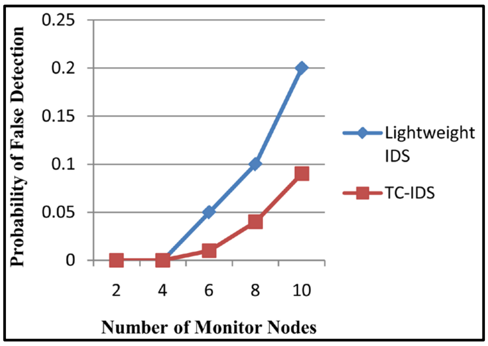

Figure 4. False detection vs. number of monitor nodes.

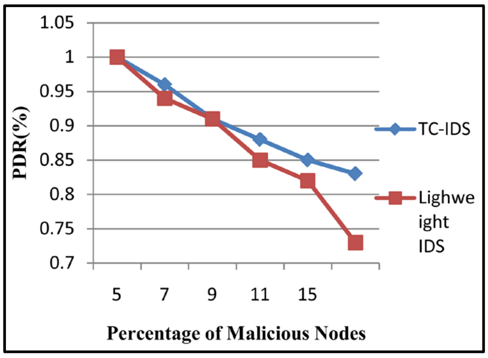

Figure 5. PDR vs. malicious nodes.

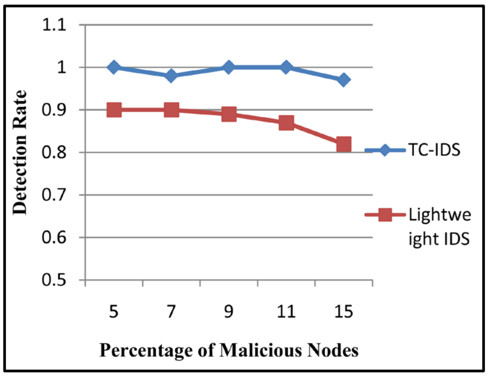

Figure 6. Detection rate vs. percentage of malicious nodes.

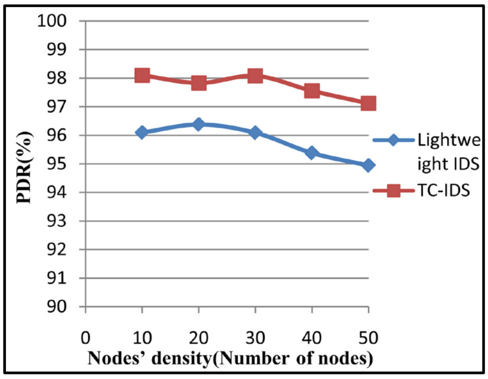

Figure 7. PDR vs. density.

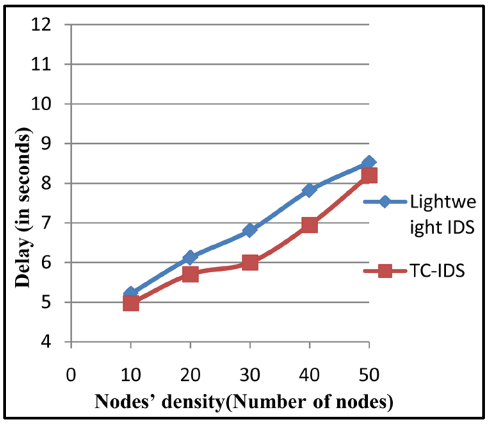

Figure 8. Delay vs. density.

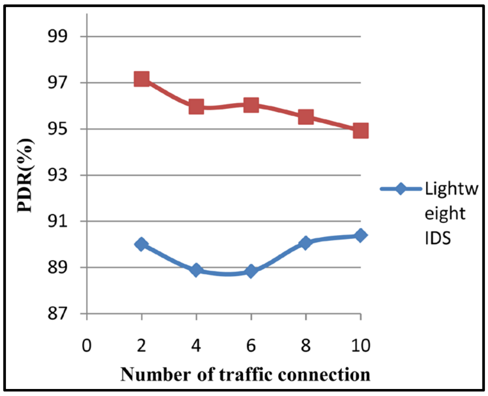

Figure 9. PDR vs. traffic.

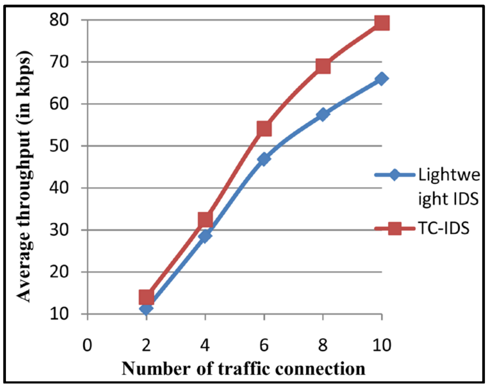

Figure 10. Throughput vs. traffic.

ments. As many of proposed security schemes are based on specific network models, lack of combined efforts to take a common model to ensure security for each layer, in future though the security mechanisms become well-established for each individual layer, combining all the mechanisms together for making them work in collaboration with each other will incur a hard research challenge.

References

[1] Townsend, C. and Arms, S. (2002) Wireless Sensor Networks: Principles and Applications. *Sensor Technology Handbook*, **11**, 575589.

[2] Pathan, A.-S.K., Lee, H.-W. and Hong, C.S. (2006) Security in Wireless Sensor Networks: Issues and Challenges.

Proceedings of 8*th IEEE ICACT* 2006, Volume II, Seon Hong, 20-22 February 2006, 1043-1048.

[3] Bhatnagar, R. and Shankar, U. (2012) The Proposal of Hybrid Intrusion Detection for Defence of Sync Flood Attack in Wireless Sensor Network. International *Journal of Computer Science & Engineering Survey*, **3**, 31-38. http://dx.doi.org/10.5121/ijcses.2012.3204

[4] Wu, J. and Li, H. (1999) On Calculating Connected Dominating Set for Efficient Routing in *Ad-hoc* Wireless Networks. *Proceedings of the* 3*rd International Workshop on Discrete Algorithms and Methods for Mobile Computing and Communication* (*DIAL'M*), Seattle, August 1999, 7-14.

[5] Haggar, B. (2009) Self-Stabilizing Clustering Algorithm for *Ad-hoc* Networks. *Proceedings of the* 5*th International Conference on Wireless and Mobile Communications*, *ICWMC* 2009, French Riviera, August 2009, 24-29.

[6] Theoleyre, F. and Valois, F. (2005) Virtual Structure Routing in *Ad-hoc* Networks. *IEEE ICC*'2005, Seoul, May 2005, 78-82.

[7] Ali, K., Sara, M., Belbachir, R., Maaza, Z.M. and Senouci, S.M. (2012) Self-Organization Framework for Mobile *Ad-hoc* Networks. *Proceedings of* 8*th International conference on Wireless Communications and Mobile Computing*, August 2012, 14-22.

[8] Krontiris, I., Benenson, Z., Giannetsos, T., Freiling, F. and Dimitriou, T. (2009) Cooperative Intrusion Detection in Wireless Sensor Networks. *Wireless Sensor Networks*, **5**, 263-278. http://dx.doi.org/10.1007/978-3-642-00224-3_17

[9] Stetsko, A., Folkman, L. and Matyas, V. (2010) Neighbor-Based Intrusion Detection for Wireless Sensor Networks. *Proceedings of International Conference on Wireless and Mobile Communications*, Los Alamitos, 420-425.

[10] Giannetsos, A. (2008) Intrusion Detection in Wireless Sensor Networks. Master's Thesis, Carnegie Mellon University, Pittsburgh.

[11] nShield Project (2012) New Embedded Systems Architecture for Multi-Layer Dependable Solutions. Project No: 269317, Selex Elsag, SE Europe.

[12] Krontiris, I., Dimitriou, T. and Freiling, F.C. (2007) Towards Intrusion Detection in Wireless Sensor Networks. *Proceedings of the* 13*th European Wireless Conference*, Paris, April 2007, 166-173.

[13] Krontiris, I., Dimitriou, T., Giannetsos, T. and Mpasoukos, M. (2008) Intrusion Detection of Sinkhole Attacks in Wireless Sensor Networks. In: *Algorithmic Aspects of Wireless Sensor Networks*, Springer, Sophia Antipolis, 150-161.

[14] Gerrigagoitia, K., Uribeetxeberria, R., Zurutuza, U. and Arenaza, I. (2012) Reputation-Based Intrusion Detection System for Wireless Sensor Networks. *Complexity in Engineering* (*COMPENG*), Aachen, 11-13 June 2012, 1-5.

[15] Krontiris, I., Giantsos, T. and Dimitriou, T. (2008) LIDeA: A Distributed Lightweight Intrusion Detection Architecture for Sensor Networks. *Proceedings of the* 4*th International Conference on Security and Privacy in Communication Networks*, ACM, Istanbul, 22-25 September 2008, 1-10.

[16] Buchegger, S. and Boudec, J.Y.L. (2003) A Robust Reputation System for Mobile *Ad-hoc* Networks. *Proceedings of P*2*PEcon*, EPFL IC Technical Report IC/2003/50.

[17] Jsang, A. and Ismail, R. (2002) The Beta Reputation System. *Proceedings of the* 15*th Bled Electronic Commerce Conference*, Bled, 17-19 June 2002, 41-55.

[18] Ganeriwal, S., Balzano, L.K. and Srivastava, M.B. (2008) Reputation-Based Framework for High Integrity Sensor Networks. *ACM Transactions on Sensor Networks* (*TOSN*), **4**, 1-7. http://dx.doi.org/10.1145/1362542.1362546

[19] Bidgoly, A.J. and Ladani, B.T. (2013) Quantitative Verification of Beta Reputation System Using PRISM Probabilistic Model Checker. *Proceedings of* 10*th International ISC Conference on Information Security and Cryptology* (*ISCISC*), Yazd, 29-30 August 2013, 1-6.

[20] Roman, R., Zhou, J.Y. and Lopez, J. (2006) Applying Intrusion Detection Systems to Wireless Sensor Networks. 3*rd IEEE Consumer Communications and Networking Conference*, *CCNC* 2006, **1**, 640-644.

[21] Patwardhan, A., Parker, J., Joshi, A., Iorga, M. and Karygiannis, T. (2005) Secure Routing and Intrusion Detection in Ad Hoc Networks. 3*rd IEEE International Conference on Pervasive Computing and Communications*, *PerCom* 2005, Kauai Island, 8-12 March 2005, 191-199.

[22] Network Simulator NS-2, 2002. http://www.isi.edu/nsnam/ns/index.html

[23] Hai, T.H., Huh, E.N. and Jo, M. (2009) A Lightweight Intrusion Detection Framework for Wireless Sensor Networks. *Wireless Communications and Mobile Computing*, **10**, 559-572.