Discrete R-Contiguous Bit Matching Mechanism Appropriateness for Anomaly Detection in Wireless Sensor Networks

M. Zeeshan, Huma Javed and Sifat Ullah

Department of Computer Science, University of Peshawar, Peshawar

***Abstract*:** Resource exhaustion is one of the main challenges for the security of Wireless Sensor Networks (WSNs). The challenge can be addressed by using algorithms that are light weighted. In this paper use of light-weighted R-Contiguous Bit matching for attack detection in WSNs has been evaluated. Use of R-Contiguous bit matching in Negative Selection Algorithm (NSA) has improved the performance of anomaly detection resulting in low false positive, false negative and high detection rates. The proposed model has been tested against some of the attacks. The high detection rate has proved the appropriateness of R-Contiguous bit matching mechanism for anomaly detection in WSNs.

***Keywords*:** Wireless Sensor Networks, R-Contiguous bit matching Security, Negative Selection, Attack Detection**.**

1. Introduction

Wireless Sensor Networks (WSNs) are specialized type of networks that has small devices called sensor nodes distributed across the network [1]. These nodes have limited memory, battery power and processing capabilities. They are deployed in large quantities to observe the phenomena of the area. The size of sensor nodes makes them feasible to observe phenomena unattended in those areas where access of human or the traditional wireless network is not possible [2, 3].However the limited resources constraint makes WSN and its application design a challenging task.

There is practically unlimited application of WSNs in the real world for monitoring the environmental [2, 4, 5], medical management [6] and many other areas. According to type of data, there is classifications of applications that must be assembled in the network. These applications could then be arranged in two different categories: event detection (ED) and spatial process estimation (SPE) [7].

With growing interest of adversaries in WSNs, the security issues turn to be more challenging. WSNs have limited energy, distributed in unattended circumstances with low computational and memory capabilities are vulnerable to various attacks. According to [8], network suffers from insider and outsider threats. In order to prevent attacks on WSNs, different approaches can be applied. However the preventive methods on some attacks have no effect [2, 3]. Also more storage and processing capabilities are required for preventive methods like encryption and authentications.

The Intrusion Detection System (IDS) provides a way to prevent adversaries to initiate malicious activities within the network [9]. However the challenges like limited energy, computation and memory limitation make traditional algorithms not applicable for WSNs. IDS for WSNs are application specific [7].

Intrusion Detection in WSN as categorized to Misuse-based, Anomaly-based and Specification-based detection. In Misuse-based detection a comparison is performed between the attack pattern. However updating of attack patterns and its storage in the memory constrained network is a challenge. Also this technique has limitation in term of novel attack detection.

However, the limitation of misuse detection is addressed in Anomaly-based detection. The focus in this technique is on normal behavior rather than attack behavior. Any deviation in the normal behavior pattern is considered anomaly. This technique has capability of detecting novel attack. However complete specification of normal profile is a challenge and partial specification will not be detecting all the novel attacks.

In Specification-based anomaly detection, limitations of misuse and anomaly based detection has been addressed. In this technique machine learning technique and training is used to define normal behavior. The specification description about what operations are allowed is done manual by human is a time consuming task and has risk of some attacks might passes undetected.

Misuse detection models have low false positive rates than anomaly detection. However this detection model works only for those attacks with known attack signature [3, 10]. Any new attack pattern or a change in the previous attack pattern with attack signature known, will remain un detected. In case of anomaly detection, the model can adjust itself by learning the profiles of normal activities [6].However for WSNs, there is need for a light weighted detection model that can detect unknown attack patterns. The algorithm needs to be intelligent and light weighted when perform matching. The Discrete-R Contiguous matching algorithm is a light weighted matching technique in which the matching of the normal against abnormal behavior is performed effectively and efficiently. It is light weighted than other matching techniques like R-Chunk and Hamming distance and is feasible for WSN, keeping in view the limited computation capabilities of sensor nodes.

2. Literature Review

Human immunology system has defense at four levels and its combination with anomaly detection takes a good effect on network securities [3, 4]. The first level of defense is the skin which stops the infection going inside [1, 2, 6, 11]. Physiological is the second level in which some conditions like PH and temperature makes antigens difficult to survive. The last level can recognize and learn an antigen is adaptive immune system [9, 12, 13].

Memory cells are generated after activation of immunocyte through the phase of clonal selection. The immunocyte that are not activated in their lifetimes will be consider as dead [4]. Threshold activation of memory cell is low whereas the life time is long. Thus the memory cells bind fewer antigens to be active and perform the detection fast [5, 6, 11].

The immunology inspired system performs complex computation in a decentralized way. Further the learned information can be called instantly and learns new information [5, 14]. Researchers have suggested immune inspired intrusion detection algorithms for Local Area Networks (LANs) because of the similarities between natural immune system and computer security [6].

The Human Immune System (HIS) can be assumed as a light-weighted distributed system with each cell having small set of tasks calibrating in a decentralized way. There are number of general purpose algorithms based on Artificial Immune System (AIS). The main concept of these algorithm is human immunology concept of distinguishing self from non-self cell. This concept is applied in IDS design to distinguish a normal packet from anomalous one. The matching mechanism used in these algorithms can be considered as the backbone of the overall model. There is always need for an intelligent matching mechanism. For WSN the matching mechanism need to be light weighted so that it shall not be a bottle neck due to limited computation capabilities of a node.

In order to simulate immune networks, a bio-inspired network model known as Idiotypic network theory (INT) is used. According to this theory molecules and lymphocytes in immune system interacting have variable regions.

One of the anomalous behavior in WSN that leads toward network congestion is the creation of routing loops in the network. The main objective of this anomaly is to increase end to end latency by replaying, spoofing and altering the rout information [2]. This scenario can stop the operations of the network due to congestion. Another anomaly can be sending faulty healthy packet to paralyze the whole network [2, 13] or to move all the traffic through an infected node [3]. In some of the anomaly a flow of traffic receiving in one part of the network is moved to other part of the network to create congestion [15]. In all the flow control anomalies in WSN, the main goal of the attacking node is to create congestion to deny services of the network. In order to achieve its goal, the anonymous node can creates multiple identities and tries to be present in different part of the network to change the flow of traffic[16, 17].

The Dendric Cell Algorithm (DCA) is known as the second generation algorithm and is immunology inspired technique for intrusion detection. This algorithms detects anomaly by taking advantage of the negative and positive feedback loops from the signal produced regarding its safe and dangerous context and further detecting anomaly signature [2, 5, 9]. The algorithm is effective for attack detection in WSN but signature storage, updating result in memory and communication are the main overheads [5, 14]. The learning capabilities are missing in this algorithm and the R-Chunk matching technique used for dangerous signal matching has high algorithmic complexity which makes it unsuitable for WSNs [2, 15]. The false positive and negative rates are high due to absence of learning capability in the algorithm which has impacted the novel attack detection rate of this algorithm[5].

An energy aware method to detect anomaly in WSNs has been devised by Drozda [18]. The algorithm uses cascading classifiers with energy cost of each increase as needed for precision in detection. The matching mechanism for anomaly detection used by this technique is R-Contiguous. However, the matching process as well as the detection is performed centrally which result in computational and computational overhead [12]. The central point of failure is one of the main challenges for this algorithm.

In Remote Password Comparison (RPC) algorithm [2] is another anomaly detection algorithm in which the verification of node ID and location is made to avoid node duplication in any part of network in WSNs. The matching mechanism used for anomaly detection is hamming distance matching. The algorithm has shown good results for novel attack detection but due to high algorithmic complexity is not suitable for WSNs. Also route repair mechanisms are also missing in this algorithm [5].

The Neighbor Listening (NL) is another immune inspired anomaly detection algorithm [2]. This algorithm allows the leader node to inform other nodes about their neighborhood. The main goal of this technique is to set channel and further to configure global channel to attacks on WSNs. One of the short come in this technique is the availability of multi-channel which results in communication overhead [4, 16]. Also the availability of channel at different node is not considered in this algorithm which leads to low detection rate for anomaly detection in WSNs.

The routing and data flow control is the responsibility of network layer of the WSN protocol stack. However, in most of the IDS, the detection of anomaly is performed at BS that can result in a single point of failure if it is compromised. There is also need for IDS design in WSN that addresses the issue of fault tolerance and light-weightiness to overcome the vulnerabilities of Hierarchical IDS architecture [13]. Most of the existing IDS are short of learning capability in the model and detection of novel attack is a challenge for them. They rely on the anomaly pattern which needs updating and this result in memory overhead for WSNs. There is need to adopt intelligent techniques that have capability of detecting novel attack with low computation [10].

Most of the existing algorithm for anomaly detection in WSNs focuses on high detection rate and ignoring the light-weightiness of the model in term of computation and communication overhead [11].

The paper is organized as: Section 2 elaborated the relevant work in intrusion detection algorithms for WSNs and immunology inspired intrusion detection algorithms. The architecture of the proposed intrusion detection system is elaborated in Section 3. Simulation of the proposed IDS is discussed in Section 4. The conclusion is drawn in Section 5.

3. Proposed Framework for Intrusion Detection with R-Contiguous bit Matching Technique

For WSNs, security has become a research challenge. However most of the research regarding security in WSNs is related to authentications or encryptions. There are very less research out comes regarding intrusion detection for WSNs.

In order to address the environmental and adoptability issues of WSNs, an immuno-inspired Anomaly Detection System (ADS) is proposed in this paper that have learning capability with intelligent and effective matching technique used. The proposed IDS can distinguish activities from attacks by learning profiles of the normal activities.

The IDS needs to detect the intrusion in a cooperative manner [19]. However, such IDS may take more training time and samples for detection accuracy. There are many papers [1, 4, 13, 17, 20, 21] regarding applicability of immuno-inspired IDS for LANs that detects intrusion in a cooperative manner. However there applicability of WSNs is not suitable due to its challenges. In WSNs; there is need of a distributed way to monitor. Secondly, resources constraint are not an issue for algorithms proposed for LANs but for WSNs heavyweight algorithms cannot be used due to limited, energy, processing and memory. Third, WSNs are more vulnerable to various attacks because of its deployment in inhospitable environments.

In order to meet WSNs special requirements for the design of IDS, a detail study of negative selection and clonal selection process resulted to propose an immuno inspired IDS.

The following are the assumptions made for the proposed IDS:

1. New nodes shall not be added into the network and nodes are stationary.
2. Tree based forwarding procedure is used for routing and directing the flow data packets towards the sink.
3. All the malicious node shows normal behavior except when making an attack
4. Before an attack start there is enough time for training.

Each sensor node has small number of neighbors in its radio range due to finite communication range of sensor nodes. A node hears messages by its detection module, from its neighbors in order to monitor behaviors of neighbors as shown in Figure 1.

The proposed IDS is divided into three phases: Self Acquisition, Detector production and Intrusion Detection.

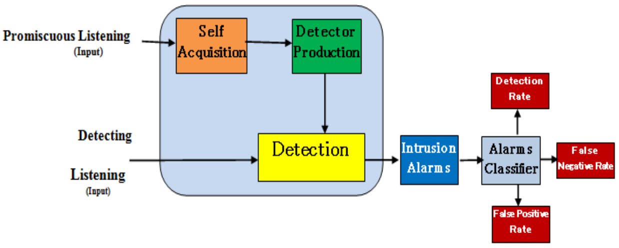


Figure 1. The Flow Control Intrusion Detection Model

3.1. Self Acquisition

During the training phase, beacons packets are retrieved from the neighbor nodes and some key parameters are extracted from them. The extracted data is stored in self pool. The extracted parameters comprises of hop count, average estimated time and parent field. The neighbor's next hop toward the sink is indicated by parent field. The jamming situation is represented by the average estimate whereas the number of hops towards the sink is defined by the hop count field. The attacker tries to affect at least one of the field to disrupt the flow of the traffic.

3.2. Detector Production

The detectors generated in this phase are stored in the detector pool. Differentiation of an attack from a normal behavior is ensured by this phase.

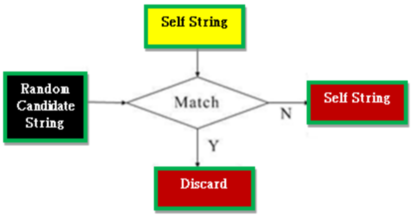


Figure 2. Negative Selection Process

Figure 2 shows the process of Negative Selection used in this phase for detector production. A mature detector is the candidate string that is random and does not match with any self strings otherwise it is rejected for being part of detector pool. Another important component of IDS is the matching rule applied in the detector production process. This rule is an integral component of detection and negative selection. The matching rule used in this research work is r-contiguous bits [7] as is illustrated below:

$$M : U \text{ x } U \rightarrow \{0, 1\}$$

$$\forall \; Si, \; Sj \; \varepsilon \; U, Si = Si1 \; Si2 \; . . . \; Sj = Sj1 \; Sj2 \; . . . \; Sjl$$

$$\left(Sik, \; Sjk \in \{0, 1\}, \; k = 1, \; 2, \ldots \; l.\right)$$

$$M\left(Si, Sj\right) = \begin{cases} 1, \; \exists k, \; 1 \le k \le l - r + 1 \; \mathbf{I}_{m=k}^{k+r-1} Sim = Sjm \\ \qquad 0, \; otherwise \end{cases}$$

The two binary strings with some length is matched with a function, M where r represents matching length of contiguous bits in the expression. U represents the set of binary string that have length l. A detector will cover fewer antigens if the value of r is greater. More detectors are needed so that the system shall have small number holes in the detector coverage [22]. Figure 3(a) elaborated the typical matching rule in which detectors are generated through a process of negative selection with bit string comprises of parent, average estimate and hop count. Figure 3 (b) illuminates discrete r-contiguous bit rule where the detectors with short bit strings are generated. Use of discrete r-contiguous bit matching mechanism decrease the size of candidate set considerably. The size of the candidate set string is 3 × 2^8 due to discrete r - contiguous rule. The matching process can be progressed by having less number of candidate strings. A sensor node can store all the candidate string because of using discrete rule that reduces the number of self string. Hole in the detector coverage will also reduce. The use of short length detectors can also lower holes in the detector coverage [5].

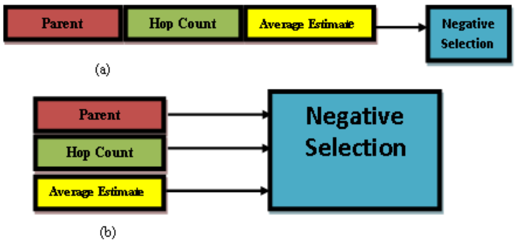


Figure 3. The discrete r-contiguous bits matching rule

The proposed algorithm meets the challenges of limited storage and processing capabilities in WSNs by using discrete r-contiguous bit matching rule which is a light weighted pattern matching technique.

3.3. Detection

The system shifts its status to detection phase just after the training period is complete and the detectors are ready. During this phase key parameters are extracted from the beacon packets which are called antigens. The detector will die if the number of matching antigens is less than the threshold that is pre-defined in the life time of detector. However, the detector will trigger an alarm if the number of matching antigens is greater than the threshold. An intrusion alarm is issued in conventional detection system as soon as the detector is active. However this procedure while detecting an intrusion takes a long time that can meet real time requirements. A fast detection procedure is implemented using discrete r-contiguous bit matching to overcome this issue. Also, whenever a malicious activity appears, the memory detectors can even trigger an alarm [16, 20].

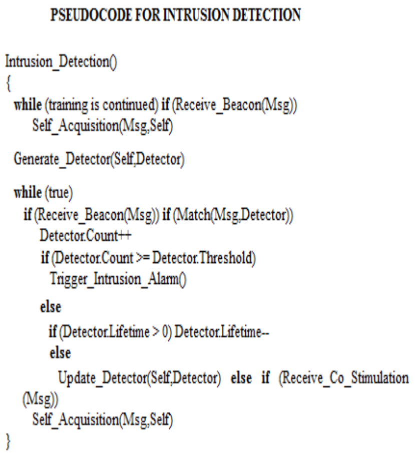
In the proposed IDS, there is less communication between neighbor node and the power utilizes results only in overhearing packets and processing the detection algorithms. The power usage is thus less than that of sending or receiving messages [5, 6, 14]

4. Discussion

The proposed IDS is simulated in OMNET++. It has a model of interference for radio simulations and has an Mica2 CC1000-based stack. The 40 nodes are distributed randomly in the simulated network with a field of 100 X 100 m^2. The radio range of each node is 80m. Every simulation starts with an attack cycles of 10000. The network has a learning period of 7200 sec in the beginning. During the training period no nodes can trigger an alarm for any detected attack. The pseudo code for proposed IDS is shown.

The adversaries start their attack after the learning period. The attack interval used is the first 20 % of an attack cycle. The network data in the simulation is fixed initially as 4 % as malicious packets that is gradually increased to check the performance. Details of the simulation parameters are shown in Table 1.

Pseudo code 1:



PSEUDOCODE FOR INTRUSION DETECTION

```
Intrusion_Detection()
{
 while (training is continued) if (Receive_Beacon(Msg))
    Self_Acquisition(Msg,Self)

 Generate_Detector(Self,Detector)

 while (true)
   if (Receive_Beacon(Msg)) if (Match(Msg,Detector))
      Detector.Count++
      if (Detector.Count >= Detector.Threshold)
        Trigger_Intrusion_Alarm()
      else
        if (Detector.Lifetime > 0) Detector.Lifetime--
        else
          Update_Detector(Self,Detector) else if (Receive_Co_Stimulation
   (Msg))
    Self_Acquisition(Msg,Self)
}
```

Table 1. Simulation Parameter

Parameters	Values
r (Matching length)	**7 bit**
Self pool size	**256 bytes**
Detector pool size	**128 bytes**
Initial lifetime	**3 cycles**
Initial threshold	**10**

In order to evaluate our proposed IDS, false positive and detection rates are calculated from the simulated environment. To evaluate the performance of proposed IDS different attacks are simulated.

Consider the scenario of evaluating Sybil attack and its detection using the proposed model shown in Figure 6. In this attack a node having multiple identities in the network is considered anomalous. The attacking node assumes the identity of another node in order to create redundancy in routing and traffic flow control. The scenario shown in the figure is designed with 40 nodes distributed randomly and using LEACH organized into different clusters. Node 31 and 35 are the cluster heads where node 0 is the base station. Each cluster head have its detectors received from the base station upon completion training. The cluster head will send each node of its locality a *HELLO* message indicating the node birth time in the network. The entire nodes respond with *RES message* with its ID, timestamp and location. Once all cluster head receives response messages from its locality, it uses the negative selection algorithm in which R-Contiguous bit matching matches the response messages received with its detectors. Upon matching an alarm message will be send to all the nodes of the locality. In the simulation shown in figure 6(b) and (c), node 17, 27 and 37 are detected sybil node. An alert message will also be sent to base station for updating the blacklist and further disseminating the information to other cluster heads of the network about the identity of anomalous nodes and its location.

The proposed model achieves 95 % detection rate for all the attacks if the self sets are full and the pool for the detectors are large enough. Figure 4 shows details of the false positive and detection rates evaluated for the five different attacks.

Some of the reasons for achieving performance are:

1. The holes in the detection coverage are reduced because of discrete r-contiguous bit matching rule.
2. Since the detectors have different coverage on the non-self set. The detector presence on each node is

complement to neighbors.

3. The detectors promoted as memory detector, validate attack signatures and thus performing detection quickly and precisely.

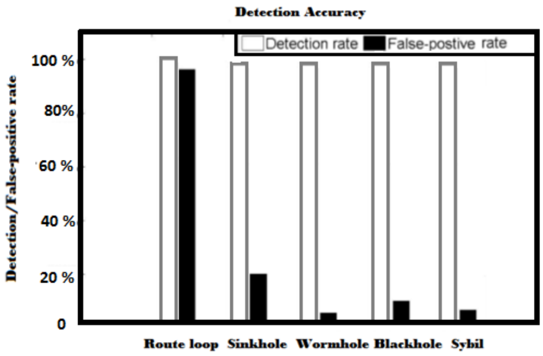


Figure 4. Detection and false-positive rates

TABLE 2. Comparison of the techniques with Sybil Attack Detection Models

Evaluation	Proposed Technique	DCA	NL	RPC
Detection Rate %	98.7	91.2	94.3	86.3
False Positive Rate %	3.2	4.2	3.5	5.6
False Negative Rate %	2.9	4.7	3.6	3.5

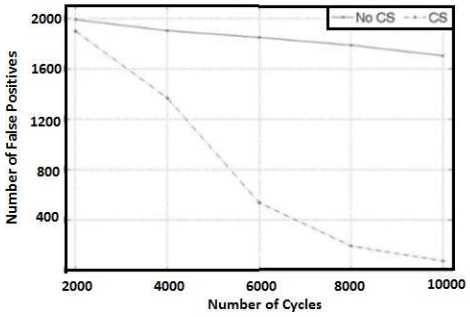
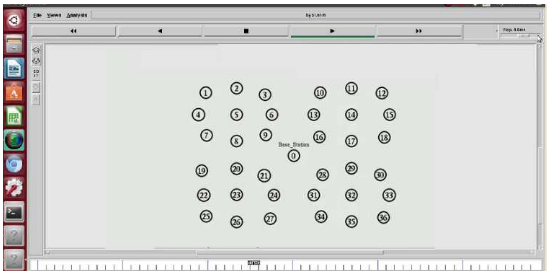
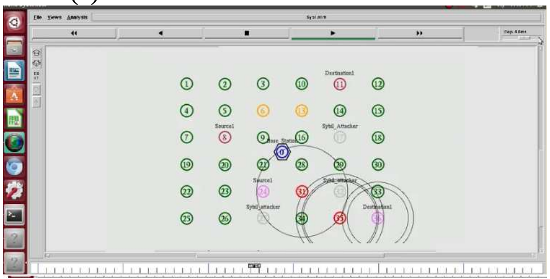


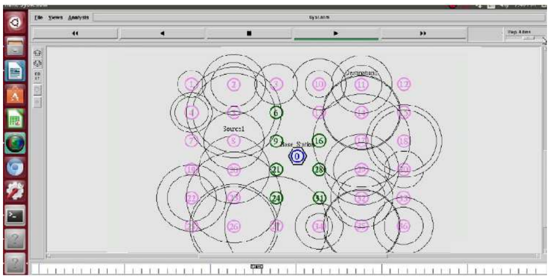
Figure 5. False positives as a function of cycles



(a). Nodes random distribution in field

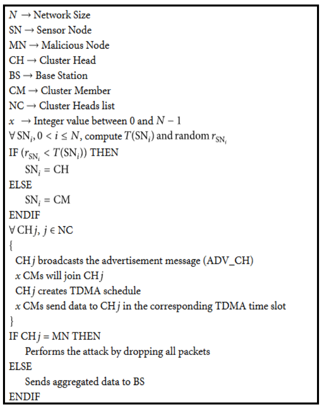


(b) Attacker detection



(c). Sybil attack detection Alarms

Figure 6. Sybil Attack Model in OMNET ++



```
$N$ → Network Size
SN → Sensor Node
MN → Malicious Node
CH → Cluster Head
BS → Base Station
CM → Cluster Member
NC → Cluster Heads list
$x$ → Integer value between 0 and $N - 1$
$\forall \mathrm{SN}_i, 0 < i \leq N$, compute $T(\mathrm{SN}_i)$ and random $r_{\mathrm{SN}_i}$
IF $(r_{\mathrm{SN}_i} < T(\mathrm{SN}_i))$ THEN
    $\mathrm{SN}_i = \mathrm{CH}$
ELSE
    $\mathrm{SN}_i = \mathrm{CM}$
ENDIF
$\forall \mathrm{CH}j, j \in \mathrm{NC}$
{
  CH$j$ broadcasts the advertisement message (ADV_CH)
  $x$ CMs will join CH$j$
  CH$j$ creates TDMA schedule
  $x$ CMs send data to CH$j$ in the corresponding TDMA time slot
}
IF CH$j$ = MN THEN
    Performs the attack by dropping all packets
ELSE
    Sends aggregated data to BS
ENDIF
```

Figure 7. Sybil Attack Model

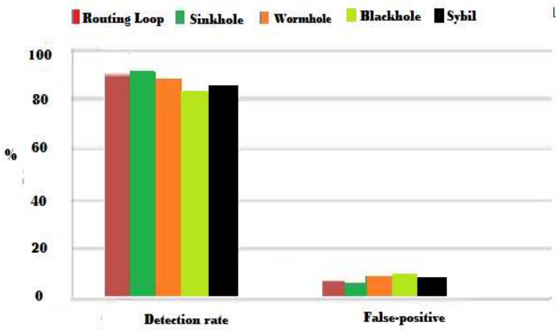


Figure 8. Detection and False-positive rates of flow control attacks

In table 2, the detection rates of different methods proposed for flow control anomaly detection are compared. The detection rate is higher for our technique with low false positive and negative rates than the other flow control anomaly detection techniques as shown in Figure 8. The DCA, RPC and NL has good performance with less number of nodes but degrades quickly as the number of nodes increases [2]. Also the detection mechanisms are computationally expensive and can be bottleneck for WSN if the field is populated with large number of nodes.

In the simulation, the number of false positives as a function of number of attack cycles is evaluated. The inspector after every 2000 cycles performs co-stimulation. Figure 5 shows the simulation results. The number of false positives decreases slowly for attacks because of the misguidance of memory detectors by network memory. The number of false positive reduces because of it. There are 74 false positives between 8000 and 10000 when the number of co-stimulation is four. This elaborates that for every 27 cycles, all the detection functions have almost one false positive.

5. Conclusions and Future works

The Sybil attack model implemented in Omnet++ is shown in figure 6 and its algorithm in figure 7. The result shows that the proposed IDS have shown satisfactory results with high detection rates and low false positives for the routing loop, sinkhole, wormhole, blackhole and sybil attacks.

The proposed IDS is also effective for detecting unknown attacks and has high accuracy as per the simulation. The numbers of false positive have been reduced due to the co-stimulation service.

This research has probed in immunity-based intrusion detection in WSNs, keeping in consideration WSN constraints. The proposed IDS keep track of updates in the network by extracting the key parameters of sensors in the network. The detection is performed distributed on each node by the detection module. Since the detection modules have different views of the networks and also complement each other which show its robustness. The immune algorithm used in the IDS has added high accuracy. The co-stimulation mechanism has resulted in decreasing the false positive rate. We are planning to extend the concept of anomaly detection system using the proposed technique for Internet of Things. The Internet of thing is secured with authentication and encryption but it cannot be protected against cyber-attacks. Thus, future research in this direction would be to develop a lightweight security mechanism which will take fewer resources for intrusion detection.

References

[1] N. K. G. Mehndi Samra, "Blackhole Attack Detection in Wireless Sensor Networks Using Support Vector Machine," *International Journal of Wireless Communications, Networking and Mobile Computing,* vol. 3, no. 5, pp. 48-52, 2016.

[2] M. Zeeshan, H. Javed, A. Haider, and A. Khan, "An immunology inspired flow control attack detection using negative selection with R-contiguous bit matching for wireless sensor networks," *International Journal of Distributed Sensor Networks,* no., 2015.

[3] A. P. R. da Silva, M. H. Martins, B. P. Rocha, A. A. Loureiro, L. B. Ruiz, and H. C. Wong, "Decentralized intrusion detection in wireless sensor networks," in *Proceedings of the 1st ACM international workshop on Quality of service & security in wireless and mobile networks*, 2005, pp. 16-23.

[4] B. Haris, "Wolf routing to detect vampire attacks in wireless sensor networks," *International Journal of Computer Science and Information Technology,* vol. 6, no. 3, pp. 2806-2809, 2015.

[5] S. Forrest, A. S. Perelson, L. Allen, and R. Cherukuri, "Self-nonself discrimination in a computer," in *Research in Security and Privacy, 1994. Proceedings., 1994 IEEE Computer Society Symposium on,* 1994, pp. 202-212.

[6] J. Balthrop, F. Esponda, S. Forrest, and M. Glickman, "Coverage and generalization in an artificial immune system," in *Proceedings of the 4th Annual Conference on Genetic and Evolutionary Computation*, 2002, pp. 3-10.

[7] Y.-C. Hu, A. Perrig, and D. B. Johnson, "Packet leashes: a defense against wormhole attacks in wireless networks," in *INFOCOM 2003. Twenty-Second Annual Joint Conference of the IEEE Computer and Communications. IEEE Societies*, 2003, pp. 1976-1986.

[8] J. D. Araújo, D. de Andrade Rodrigues, L. S. de Melo, and Z. Abdelouahab, "EICIDS-elastic and internal cloud-based detection system," *International Journal of Communication Networks and Information Security,* vol. 7, no. 1, p. 34, 2015.

[9] S. Shamshirband, N. B. Anuar, M. L. M. Kiah, V. A. Rohani, D. Petković, S. Misra, *et al.*, "Co-FAIS: cooperative fuzzy artificial immune system for detecting intrusion in wireless sensor networks," *Journal of Network and Computer Applications,* vol. 42, no., pp. 102-117, 2014.

[10] C. Karlof and D. Wagner, "Secure routing in wireless sensor networks: Attacks and countermeasures," *Ad hoc networks,* vol. 1, no. 2, pp. 293-315, 2003.

[11] P. D'haeseleer, S. Forrest, and P. Helman, "An immunological approach to change detection: Algorithms, analysis and implications," in *Security and Privacy, 1996. Proceedings., 1996 IEEE Symposium on*, 1996, pp. 110-119.

[12] J. Timmis, P. Andrews, N. Owens, and E. Clark, "An interdisciplinary perspective on artificial immune systems," *Evolutionary Intelligence,* vol. 1, no. 1, pp. 5-26, 2008.

[13] H. Soleman and A. Payandeh, "Self-protection mechanism for wireless sensor networks," *International Journal of Network Security & Its Applications*, vol. 6, no. 3, p. 85, 2014.

[14] I. Onat and A. Miri, "An intrusion detection system for wireless sensor networks," in *Wireless And Mobile Computing, Networking And Communications, 2005.(WiMob'2005), IEEE International Conference on*, 2005, pp. 253-259.

[15] D. Dasgupta and F. González, "An immunity-based technique to characterize intrusions in computer networks," *IEEE Transactions on Evolutionary Computation,* vol. 6, no. 3, pp. 281-291, 2002.

[16] E. Karapistoli and A. A. Economides, "ADLU: a novel anomaly detection and location-attribution algorithm for UWB wireless sensor networks," *EURASIP Journal on Information Security,* vol. 2014, no. 1, p. 3, 2014.

[17] D. E. Denning, "An intrusion-detection model," *IEEE Transactions on software engineering*, no. 2, pp. 222-232, 1987.

[18] I. Onat and A. Miri, "A real-time node-based traffic anomaly detection algorithm for wireless sensor networks," in *Systems Communications, 2005. Proceedings*, 2005, pp. 422-427.

[19] N. Jeyanthi, N. C. S. Iyengar, P. M. Kumar, and A. Kannammal, "An enhanced entropy approach to detect and prevent DDoS in cloud environment," *International Journal of Communication Networks and Information Security,* vol. 5, no. 2, p. 110, 2013.

[20] V. Shnayder, M. Hempstead, B.-r. Chen, G. W. Allen, and

M. Welsh, "Simulating the power consumption of large-scale sensor network applications," in *Proceedings of the 2nd international conference on Embedded networked sensor systems*, 2004, pp. 188-200.

[21] P. Levis, N. Lee, M. Welsh, and D. Culler, "TOSSIM: Accurate and scalable simulation of entire TinyOS applications," in *Proceedings of the 1st international conference on Embedded networked sensor systems*, 2003, pp. 126-137.

[22] L.-m. Sun, J.-z. Li, and Y. Chen, "Wireless sensor networksTsinghua University Press," *Beijing, China*, 2005.