An Architecture for Resilient Intrusion Detection in IoT Networks

Mohammed Al Qurashi
Bournemouth University
Poole, Dorset, UK
malqurashi@bournemouth.ac.uk

Constantinos Marios Angelopoulos
Bournemouth University
Poole, Dorset, UK
mangelopoulos@bournemouth.ac.uk

Vasilios Katos
Bournemouth University
Poole, Dorset, UK
vkatos@bournemouth.ac.uk

Abstract—**We introduce a lightweight architecture of Intrusion Detection Systems (IDS) for ad-hoc IoT networks. Current state-of-the-art IDS have been designed based on assumptions holding from conventional computer networks, and therefore, do not properly address the nature of IoT networks. In this work, we first identify the correlation between the communication overheads and the placement of an IDS (as captured by proper placement of active IDS agents in the network). We model such networks as Random Geometric Graphs. We then introduce a novel IDS architectural approach by having only a minimum subset of the nodes acting as IDS agents. These nodes are able to monitor the network and detect attacks at the networking layer in a collaborative manner by monitoring 1-hop network information provided by routing protocols such as RPL. Conducted experiments show that our proposed IDS architecture is resilient and robust against frequent topology changes due to node failures. Our detailed experimental evaluation demonstrates significant performance gains in terms of communication overhead and energy dissipation while maintaining high detection rates.**

I. Introduction

Internet of Things is an emerging networking paradigm enabling computers and people, *things* and *machines* to seamlessly exchange information and data over the Internet. By 2025 around 55 billion IoT devices will be deployed and more than 15 USD trillion will be invested in IoT in aggregate between 2017 and 2025 [1]. IoT is already being deployed in many critical settings and environments such as healthcare, manufacturing, critical infrastructure [2], and so forth. IoT in the modern economy has been targeted by malicious actors due to the lack of security measures. A representative example is that of the Mirai botnet [3] or the incident where hackers were able to take over and control the steering and braking systems of a Jeep car [4].

Cyber security controls can be clustered in three layers. The first layer consists of preventive countermeasures such as authentication and access control mechanisms, cryptography , firewalls, etc. The second layer (also known as the second line of defence) consider detection countermeasures that are engaged *during* an attack, such as Intrusion Detection Systems. Finally, at the last layer lie recovery measures and processes for post-incident management, such as security information incident management and digital forensics. Due to the inherent and particular characteristics of IoT (i.e. highly constrained devices, deployed in big numbers with ephemeral availability), the corresponding cyber security measures need to be revisited.

In the domain of Intrusion Detection Systems (IDS) for IoT environments, a considerable body of research exists on deployment architectures, detection strategies and algorithms. However, available IDS in IoT are designed based on assumptions holding from "conventional" computer networks, e.g. that each node of the network is assumed to be powerful in terms of resources (available energy, memory, CPU, etc.). They are also assumed to be always available and the nodes to communicate over a reliable and high-capacity network. An IDS that efficiently addresses the IoT paradigm is needed.

A wireless sensor actuator network (WSAN) consists of a set of nodes, called sensors, deployed over an area of interest. The devices communicate over the air with their peers, collaboratively carrying out complex tasks. WSNs are a key enabling technology for the IoT and as such share several common characteristics. Therefore, WSNs have provided an ideal R&D platform for several IoT protocols and technologies, such as CoAP and 6LoWPAN [5].

Our contribution. We introduce a hybrid IDS architecture for IoT networks that consists of centralized and distributed IDS agents integrated with a novel placement strategy. In our approach, the IDS architecture can detect and mitigate the effect of node failures. Firstly, we model a WSN with the use of Random Geometric Graphs (RGG). The RGG model can formally express the spatial characteristics of the network such as network connectivity, by capturing the inter-dependencies and the existence of wireless links among neighbouring nodes. Then, motivated by how IoT networking protocols, such as RPL, manage and operate the network, we identify the trade-offs between the communication overheads introduced by an IDS and its detection rate of attacks such as the sinkhole attack. We investigate this trade-off via extended emulations and show that it is not necessary for all nodes to act as IDS agents. Furthermore, we show that the proposed architecture is able to efficiently cope with and mitigate the effects of nodes failures on the the efficiency of the IDS.

The rest of the paper is organised as follows. Section 2 presents the current state-of-the-art with a special emphasis on the most important contributions in Intrusion Detection Systems in WSNs. Sections 3 and 4 introduce the proposed network model and adopted IDS architecture based on Random Geometric Graphs. Section 5 presents the performance evaluation of the proposed approach and discusses the simulation results and findings. Finally, conclusions are discussed in Section 6.

II. Related Work

Over the past few years, Intrusion Detection Systems for WSNs and the IoT have attracted significant research interest. IDSs can be classified based on their architecture, namely centralised, distributed or hybrid. In centralized IDSs, the detection algorithms are executed and performed on a designated node (host). The necessary monitoring and detection data have to be reported to a centrally located base station which is assumed to be powerful in terms of processing capabilities and available memory and energy. In a distributed architecture on the other hand, each individual network node runs an IDS agent cooperatively with other agents in the network. Finally, hybrid IDS architectures demonstrate a combination of the centralised and distributed architectures in an effort to avoid the disadvantages of each individual approach.

In [6], the authors proposed a detection method for WSNs that integrates with intrusion prevention system. In this approach, symmetric encryption and oneway hash function have been used to construct the routing path between the BSs and nodes. Their results showed that the total amount of required energy can be reduced. However, the use of symmetric key increases the computation overheads. In [7], the authors proposed an intrusion detection system for IoT named Kalis. Kalis is placed at the border router to collect features of the network and use these to dynamically configure appropriate detection techniques. The authors claim that this approach can be applied and extended to new protocols as it is independent of the detection method.

In [8], the authors proposed a centralised intrusion detection system for IoT. They introduced Complex Event-Processing (CEP) techniques to monitor network packets that is placed at the router border. The experimental results reveal that their approach yields increases in the computation overheads but consumes less memory compared to traditional IDS.

In [9], the authors proposed a distributed anomaly detection method for WSNs that uses in-network hierarchical processing. The nodes of the network are first clustered using fuzzy c-means clustering, and then run an incremental model to score local and global outliers. The results showed that this distributed method can achieve high detection accuracy and smaller computational communication overheads. In [10], authors proposed a segment-based anomaly detection method to detect anomalies in WSNs. This algorithm has combined the Distributed Segment-Based and KullbackLeibler divergence measures and distributed the sensor nodes in clusters and each cluster has cluster head node. This proposed detection method limited to hierarchical network and my applied for flat network with additional requirements.

In [11], the authors proposed a distributed signature-based detection system for IoT. The adopted detection algorithm in each node matches against conventional attacks signatures in Snort. Their detection approach may detect attacks faster than other algorithms, but only detects known conventional attacks.

In [12], the authors introduced an IDS for WSN that follows a hybrid architecture. Their solution focuses on routing attacks and consists of a central IDS module (running computationally intensive processes) that runs on the Sink node and a lightweight distributed agent that is deployed on sensor motes. The proposed IDS has three main modules: a central module called mapper, a lightweight intrusion detection module, and a firewall. The proposed solution shows a good performance in small networks, but it introduces a massive communication overhead in larger networks. This is mainly due to the fact that the lightweight agent is deployed on every single sensor mote of the network, thus leading to bottleneck phenomena to emerge around the Sink as the diameter of the network increases. In [13], the authors proposed a hybrid IDS for IoT by extending [12]. They extended the detection module of SVELTE by using ETX (Expected Transmissions) metric within the detection procedure. Their empirical evaluation revealed that their approach achieved high detection rates. However, they evaluated their approach in small networks with few nodes. Further,in [14], the authors proposed a specification-based intrusion detection system for IoT to detect attacks on RPL-based networks. Their approach is based on hybrid and partly distributed architecture that divides the network into clusters where each cluster has a cluster head. The simulation results revealed that their approach achieved high detection rate and low overhead. However, this proposed IDS is limited to cluster based networks.

The current state-of-the-art on IDSs for WSN and IoT networks are still resource-intensive, as it is primarily stemming from assumptions holding from conventional computer networks. Centralised IDS architectures introduce significant communication overhead to the network as the base station (or Sink) due to large numbers of requests to and from the nodes related to IDS data collection. Distributed IDS architectures rely on the cooperation among the sensor nodes, thus increasing the communication load as well as energy dissipation. Lastly, hybrid IDS architectures achieve a better control and global overview of the network, but currently available solutions also introduce a significant communication overhead that increases proportionally to the number of network nodes. Furthermore, the resilience and robustness have not been studied yet.

In this work we focus on hybrid IDS architectures but we show that by taking into account the specifics of IoT protocols, such as the ranking mechanism of RPL, as well as the spatial characteristics of such networks, the number of required IDS agents in the network (and therefore the corresponding overhead) can be greatly reduced while maintaining sufficiently high detection rates.

III. The Network Model

Internet of Things envisions the massive connection of embedded systems, smart devices and things over the Internet. Wireless Sensor & Actuator Networks (WSANs), known as a key enabling technology for IoT, are found in several IoT systems. WSANs consist of a number of tiny devices equipped

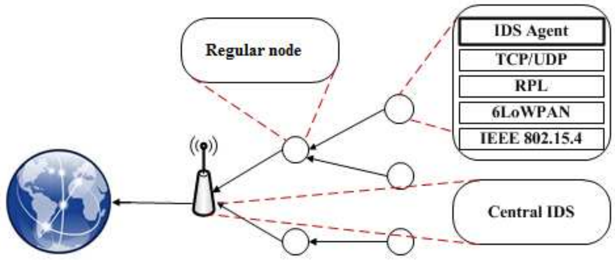


Fig. 1: The Proposed Architecture

with sensors monitor specific environmental variables (e.g. ambient luminance, temperature, etc). Each sensor is a fully-autonomous computing and communication device, characterized by its constrained nature in terms of available power supply, transmission range r, limited processing power and memory capabilities. In this work we focus our study on WSANs where the sensors are static and are deployed over the network area uniformly at random.

The Base Station, also called the Sink, represents the border gateway device lying on the edge of the WSAN network. It initiates the self-organisation of the network. The sink node is assumed to be powerful in terms of computational resources and capabilities, memory and energy supplies.

In this work, we consider the random placement of the sensor nodes in the network area by a *Random Geometric Graph* (RGG). RGG are constructed by n vertices that are placed at random in the area of interest [0,1]^2. An edge (u, v) exists iff the Euclidean distance of vertices u and v is at most r, where r is the radius (wireless communication range) r of the sensors. RGG represents a realistic model for WSANs since it captures the extent of the communication structure of real networks such as the spatial aspects.

Particularly, we consider an area $\mathcal{A} \subset \mathbb{R}^2$ in two dimensional space. An instance of the *random geometric graphs model* $\mathcal{G}(\mathcal{X}_n; r)$ is constructed as follows: for n points $\mathcal{X}_n$ uniformly placed at random in $\mathcal{A}$. The set $V = \mathcal{X}_n$ is the set of vertices of the graph and we connect two vertices iff their euclidean distance is at most r. For any vertex $v \in V$ we denote by $N(v)$ the set of neighbours of v and by $\deg(v) = |N(v)|$ its degree. Further, we denote by $\|u-v\|$ the Euclidean distance between the points corresponding to vertices v, u. RGG model provides us with a formal tool of constructing and characterising networks as "*sparse*", "*dense*" or "*normal*".

IV. The Proposed IDS

We propose a hybrid architecture of an Architecture Intrusion Detection System that consists of a central detection agent located in the base station and a distributed lightweight intrusion detection agent deployed on a subset of the network nodes as shown in Figure 1. The central IDS controls the entire IDS architecture and relevant data from the distributed agents. Each network node that runs an instance of the distributed agent, monitors and collects data on local network activity from its 1-hop neighbouring nodes. This implies that not all nodes need to run the IDS agent, but only a subset of them such that every node in the network has at least one 1-hop neighbour operating as IDS agent. In graph theory, such a subset is defined as a vertex cover of the corresponding RGG graph that captures the structure of the network. In our approach (algorithm 1), the subset of the nodes that act as IDS agents is selected based on the Vertex-cover algorithm [15] (greedy algorithm) to find a subset of minimum cardinality with proper placement. Moreover, we propose a method to maintain and monitor the distributed IDS agents against node failures. As shown in Algorithm 1, the central IDS frequently checks the set of IDS agents against node failures. In case any of the IDS nodes fail to communicate with the central IDS, the central IDS agent will re-run our proposed algorithm to select a new subset of the nodes to act as IDS agents.

Algorithm 1 Detect Sinkhole Attacks

```
Require: $N \leftarrow$ the list of nodes
Require: $S \leftarrow$the list of neighbour nodes
Require: $A \leftarrow$ the list of selected Node to run as an IDS agent
Require: $A' \leftarrow$ A
while $A = \emptyset$ OR $A \neq A'$ do
    while $N \neq \emptyset$ do
        Select a set of neighbours $\in S$ that maximise $S \cap N$
        $N \leftarrow N - S$
        $A \leftarrow A \cup \{S\}$
        $A' \leftarrow A$
        return $A, A'$
    end while
end while
for Node in A do
    for Node in S do
        if (Node.Rank+IDSagentNodeRank
< Node.Parent.rank) then
            Node.fault++
        end if
    end for
end for
for Node in N do
    if Node.fault>Threshold then
        Raise Alarm
    end if
end for
```

We apply our aforementioned approach by extending the state of the art IDS for WSN by Raza et al. called SVELTE [12]. In SVELTE, authors consider multi-hop peer-to-peer IPv6-enabled WSNs running the 6LoWPAN stack [5] on ContikiOS [16]. They develop a hybrid IDS architecture that consists of a centralized module running on the Sink and a distributed agent running on each individual sensor node. The centralized module contains the 6LoWPAN Mapper (6Mapper) which gathers information from the sensor nodes on the network topology. In particular, 6Mapper collects information on the rank assigned to each node by the RPL protocol which is closely related to the hop distance of each node from the Sink. This allows IDS agents to monitor their immediate neighbouring nodes against anomalies. For instance, a sinkhole attack could be performed by having malicious or compromised nodes falsely announcing to their neighbours a significantly lower rank than the actual one. Thus, all network traffic would go through the malicious node.

RPL establishes and maintains routing paths between the Sink and the rest of the network nodes by constructing a global network topolog using the Destination Oriented Directed Acyclic Graph (DODAG). The Sink initially broadcasts exploratory messages to its immediate neighbouring nodes, which in turn reiterate the process to their neighbouring nodes lying further away in the network. The process is run recursively and eventually results in each node being assigned a rank that depends on its actual hop-distance to the Sink as well as the link quality between neighbouring nodes (as measured by an objective function, such as the ETX metric). In SVELTE, the 6Mapper periodically collects these ranks to reconstruct the DODAG centrally at the Sink in order to monitor the network against relevant attacks - like sinkhole - by detecting corresponding anomalies as shown in Algorithm 1; for example, if the rank of a node significantly deviates from the rank of its neighbours.

While each individual node introduces a small communication overhead (6Mapper requests are 5 bytes long while each response from the nodes is 17 bytes long), engaging all nodes in the process introduces a significant communication overhead that is proportional to the size of the network. This poses significant scalability issues and adversely affects the connectivity and availability of the network as in multi-hop peer-to-peer networks nodes closer to the Sink also serve traffic coming from the rest of the network.

The main idea of our approach is that networking protocols designed to address the distributed ad-hoc nature of IoT networks use local network information available to the nodes such as RPL. This network information can be monitored by 1-hop neighbouring nodes. Therefore, for a given set of neighbouring nodes it suffices that only one of them is actively collecting and reporting relevant information to the Sink. This greatly reduces the number of nodes that need to operate as IDS agents, thus mitigating any scalability and performance issues.

In this work we focus on experimentally evaluating our approach on SVELTE as a representative example of a hybrid IDS architecture for ad-hoc networks. Particularly, we evaluate the trade-off between the potentially reduced overhead of the IDS and potential drop in the detection rate (due to the lower number of active IDS agents in the network) versus the reduced communication overheads and increased energy efficiency of the network. We also evaluate the resilience and robustness of our proposed method against random node failures.

V. Performance Evaluation

A. Simulation Set-Up

We ran our experiments in two parts. Firstly, we evaluate the efficiency and effectiveness of our proposed approach. Then, we study the resilience and redundancy of the proposed architecture. For both experiments we use Cooja [17], which provides a detailed cross-layer simulation for WSNs running the 6LoWPAN stack. We consider three qualitatively distinct network densities as these are indicated by the Random Geometric Graph model. Particularly, we consider a network area $\mathcal{A} = [0, 100]^2$ where n sensor motes are deployed uniformly at random, for $n \in \{32, 64, 128\}$. We get three network set ups where r is (a) almost equal to; (b) $\times 1.5$ and (c)$\times 2$ the connectivity threshold, thus resulting in (a) *sparse*, (b) *normal* and (c) *dense* networks.

For each network density, we consider our approach algorithm 1 where the nodes acting as IDS agents selected based on cover set algorithm,namely, greedy algorithm. With each case we set 10% of the node population to act as malicious nodes deploying sinkhole attacks by exploiting the rank mechanism of RPL. Any remaining nodes are regular nodes. Furthermore, in the second part of our experiment we gradually drop off some nodes that perform IDS agent during the simulation to evaluate the redundancy of our approach.

For each network configuration we also run a scenario with no nodes operating as IDS nodes. For each scenario we create 10 random instances of the network; this allows us to effectively mitigate in our simulations any issues that might occur due to the random network topology (in other words we sample the space of RGG instances). For each instance we run 10 iterations of simulating the network operation for a simulation time of 3600 seconds where nodes generate and transmit data approximately every second. For each scenario and each performance metric we compute average values and 95% confidence intervals.

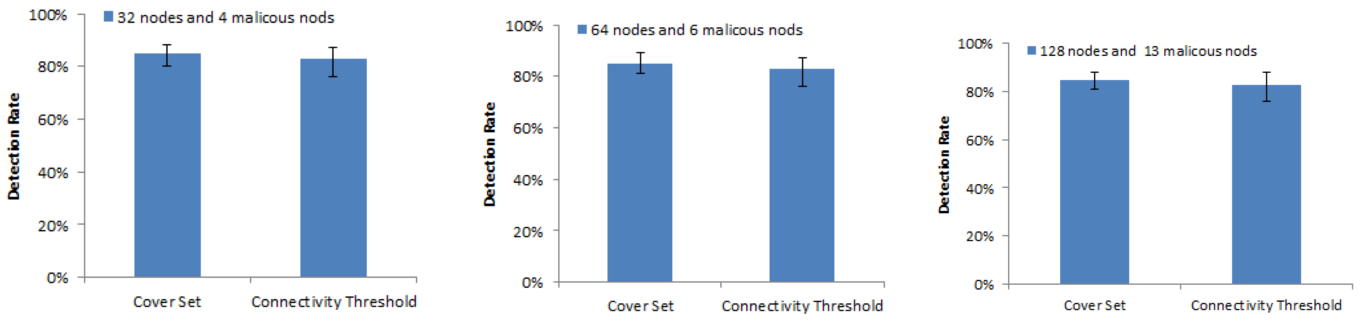
B. Evaluation Metrics

In the following subsections we define the metrics that are used to evaluate our proposed IDS architecture.

1) Detection Rate: We define the detection rate as the number of true positive detections of malicious nodes over the total number of malicious nodes in the network.

$$\text{Detection rate} = \frac{\text{number of true positive detections}}{\text{total number of malicious nodes}} \quad (1)$$

2) Communication Overhead: We define the communication overhead as the additional volume of data communication introduced in the network as a result of the operation of the IDS. We follow the practise of [12] and monitor this metric only to the 1-hop neighbouring nodes of the Sink (the rationale is that any network traffic will have to go through these nodes prior to reaching the Sink). We denote by E_{IDS} the energy consumption of the said nodes with the IDS running and with $E_{\overline{\text{IDS}}}$ the energy consumption of the said nodes with no IDS running in the network. Then,

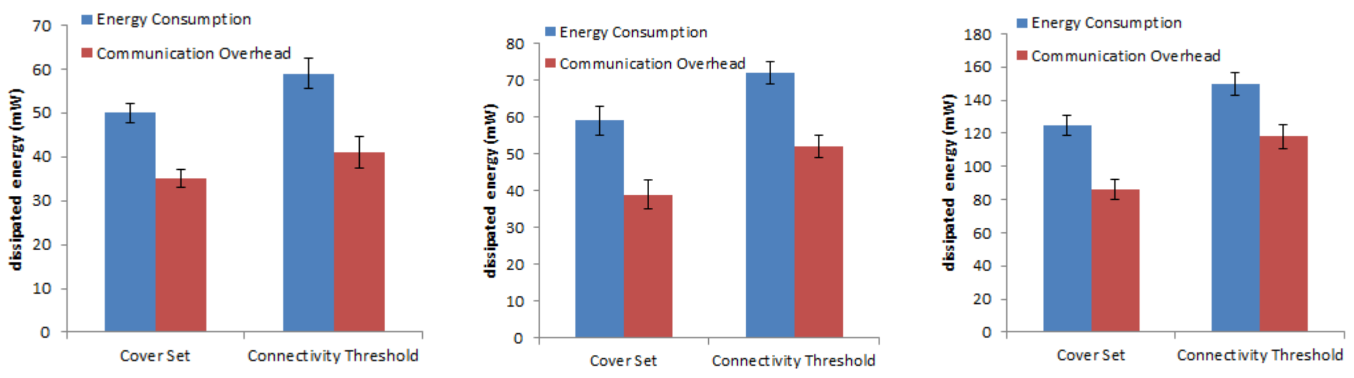


(a) Sparse network

(b) Normal density network

(c) Dense network

Fig. 2: IDS detection rate

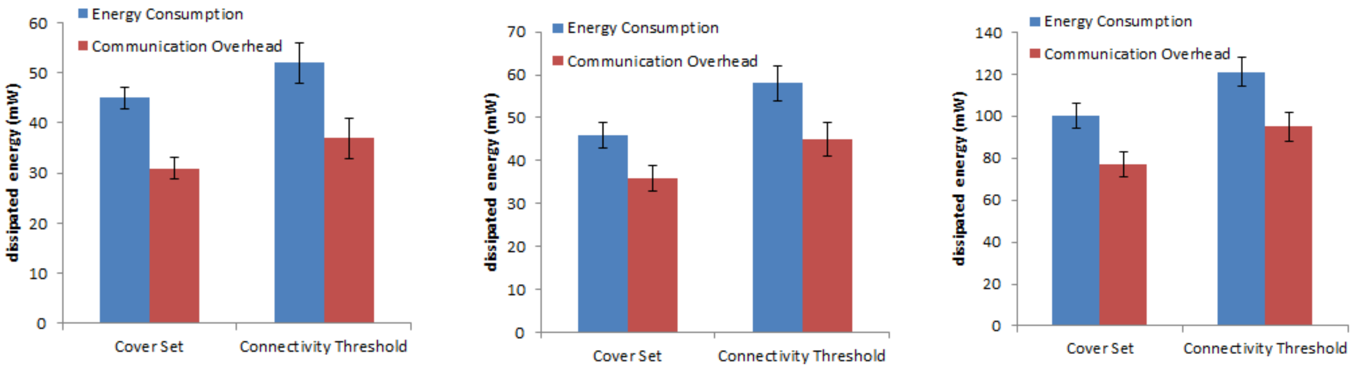


(a) Sparse network

(b) Normal density network

(c) Dense network

Fig. 3: Energy consumption and communication overhead for the entire network



(a) Sparse network

(b) Normal network

(c) Dense network

Fig. 4: Energy consumption and communication overhead introduced by the IDS

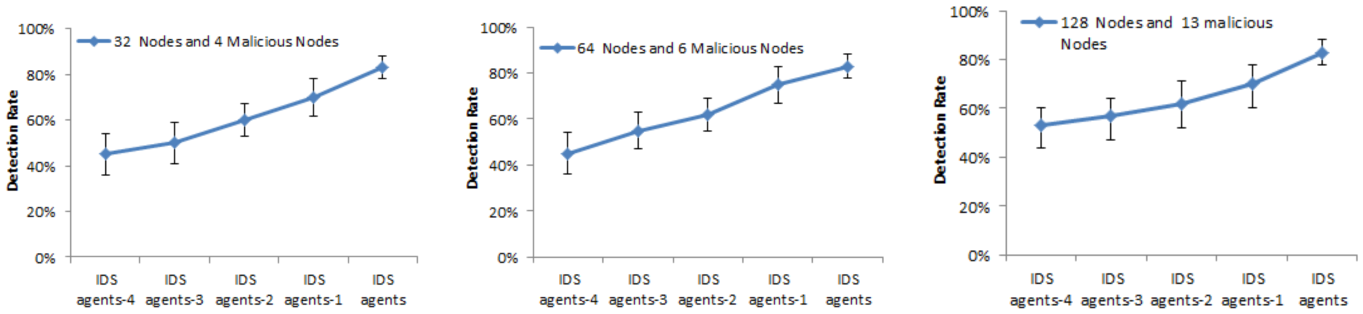
$$\text{Communication overhead} = \frac{E_{\text{IDS}} - E_{\overline{\text{IDS}}}}{E_{\overline{\text{IDS}}}} \qquad (2)$$

3) Total Energy Consumption in the Network: We measure the total energy consumption ΔE_{total} in the network as the difference between the total available energy in the network at the beginning of a simulation and at the end. We denote initial available energy for sensor i by E^i_{init} and the initial available energy for sensor i by E^i_{final}. Then,

$$\Delta E_{total} = \Sigma_{i \in n}(E^i_{\text{init}} - E^i_{\text{final}}) \qquad (3)$$

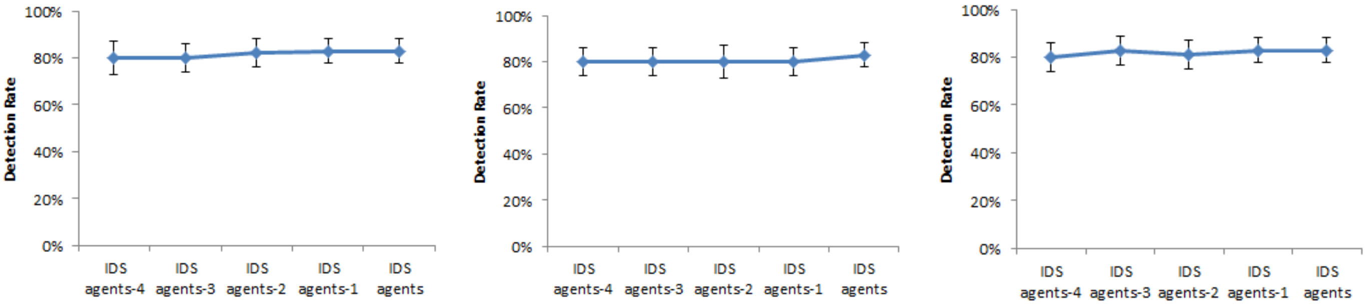
C. Simulation Findings

Figure 2 shows that in all network densities the average of detection rate where the subset of the node population operates as an IDS agent selected by our approach that uses cover set (greedy algorithm) remains high, around 80%. Also, the detection rate in random placement of distributed IDS agents



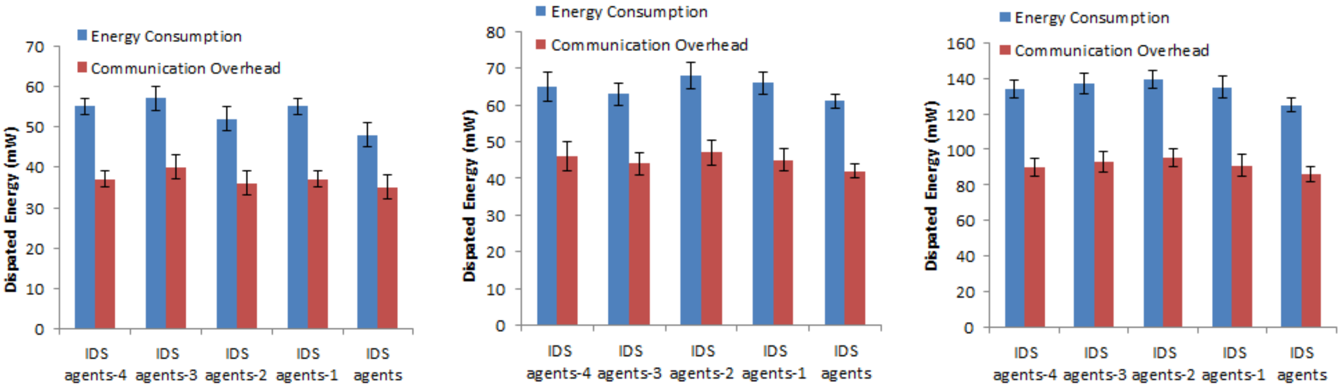
(a) Sparse network (b) Normal density network (c) Dense network

Fig. 5: Detection rate over IDS agent node failure



(a) Sparse network (b) Normal density network (c) Dense network

Fig. 6: Detection rate after IDS agents failure recovery



(a) Sparse network (b) Normal density network (c) Dense network

Fig. 7: Energy consumption and communication overhead introduced by the IDS with recovery mechanism

based on connectivity threshold [18] remains as high as 85%. However, in very rare cases areas of the network remain unmonitored because of the random placement of IDS agents. This demonstrates that our approach provides better placement of distributed IDS architecture since it allows the proper nodes to perform the IDS agent.

Figures 3 and 4 show that the energy consumption and the communication overhead introduced to the network by the IDS is proportional to the number of nodes operating as IDS agents. This shows that our approach achieved lower communication overhead and energy consumption rate compered to random placement [18] based on connectivity threshold where a constant number of nodes performing the IDS agent. Moreover, figures 2 and 3 show that our approach achieved high detection rate with lower energy consumption which reveals that minimal number of nodes were allowed to run the IDS agent.

At the second part of our experiment, first, we drooped off gradually and arbitrarily some IDS agent nodes during the simulation to study the resilience and how that effect the efficiency of our approach. Figures 5 show that the detection rate quickly drops due to that areas of the networks when nodes were drooped off left un-monitored. Then, we evaluated our algorithm that integrated with our approach that monitors the health of IDS agents.We also, dropped off gradually and arbitrary some IDS agent nodes during the simulation. Figure 6 shows that the detection rate remains high even after the nodes dropping which indicates that our approach provides a level of resilience against nodes failure.

Figure 7 shows that for all network densities the energy consumption and the communication overhead introduced to the network by our proposed algorithm that monitors the distributed IDS agents against nodes failure. The energy consumption slightly increased after random IDS agents nodes drooping due to that centralised IDS reallocate the distributed IDS agents in order to recover the area that left un-monitored. It is worthwhile the effort that provides the resilience of distributed IDS architecture against node failures.

This indicates that the energy efficiency and resilience of hybrid IDS architecture for ad-hoc networks is independent to the number of nodes acting as IDS agents and their placement. It suffices that only one of neighbouring nodes monitors and reports relevant information to the Sink. Thus, it reduces the number of nodes that are needed to operate as IDS agents.

VI. Conclusions and Future Work

In this work we study efficient and lightweight Intrusion Detection Systems for ad-hoc networks via the prism of IPv6-enabled Wireless Actuator Sensor Networks. We first use Random Geometric Graphs (RGG) that allows to provide a formal model of WSNs. RGG capture the spatial characteristics of WSNs as such interdependencies on the existence of wireless links among neighbouring nodes. We focus on network attacks in IoT-specific networking protocols such as sinkhole attack in RPL. We identify the underline cause of communication overhead in state-of-the-art and try to optimise the trade-off between energy efficiency of IDS and detection rate. We propose a novel IDS architecture that requires only a subset of the nodes with proper placement to efficiently operate distributed IDS agents.

We integrate our method on the state of the art on IDS for WSNs and conduct our performance evaluation via extensive emulations. We consider various network densities as they are formally defined by RGG model. Experiment results show that our proposed approach achieved high detection rates with a subset of the nodes running as IDS agents. The energy consumption and communication overhead introduced by the IDS reduced since the energy consumption is proportional to the number of IDS agents. Furthermore, results show that our proposed IDS architecture is resilient and robust against node failures. Centralised IDS monitors the distributed IDS agents and reallocates a new subset to run as IDS agents whenever node failure accrues.

In our future work we will employ our method on real-world network structured instead of random placement of nodes. We will also work in providing efficient algorithms as balancing the overhead among all the nodes.

Acknowledgement

This work has received funding from the European Unions Horizon 2020 research and innovation program under the grant agreement no 830943 (ECHO).

References

[1] Statista. (2018) Size of the internet of things market worldwide in 2014 and 2020, by industry (in billion u.s. dollars). [Online]. Available: https://www.statista.com/statistics/512673/worldwide-internet-of-things-market/

[2] S. Li, L. Da Xu, and S. Zhao, "The internet of things: a survey," *Information Systems Frontiers*, vol. 17, no. 2, pp. 243–259, 2015.

[3] C. Kolias, G. Kambourakis, A. Stavrou, and J. Voas, "Ddos in the iot: Mirai and other botnets," *Computer*, vol. 50, no. 7, pp. 80–84, 2017.

[4] T. Ring, "Connected cars–the next targe tfor hackers," *Network Security*, vol. 2015, no. 11, pp. 11–16, 2015.

[5] Z. Shelby and C. Bormann, *6LoWPAN: The wireless embedded Internet*. John Wiley & Sons, 2011, vol. 43.

[6] S. Y. Moon, J. W. Kim, and T. H. Cho, "An energy-efficient routing method with intrusion detection and prevention for wireless sensor networks," in *Advanced Communication Technology (ICACT), 2014 16th International Conference on*. IEEE, 2014, pp. 467–470.

[7] D. Midi, A. Rullo, A. Mudgerikar, and E. Bertino, "Kalisa system for knowledge-driven adaptable intrusion detection for the internet of things," in *Distributed Computing Systems (ICDCS), 2017 IEEE 37th International Conference on*. IEEE, 2017, pp. 656–666.

[8] C. Jun and C. Chi, "Design of complex event-processing ids in internet of things," in *2014 Sixth International Conference on Measuring Technology and Mechatronics Automation*. IEEE, 2014, pp. 226–229.

[9] H. Kumarage, I. Khalil, Z. Tari, and A. Zomaya, "Distributed anomaly detection for industrial wireless sensor networks based on fuzzy data modelling," *Journal of Parallel and Distributed Computing*, vol. 73, no. 6, pp. 790–806, 2013.

[10] M. Xie, J. Hu, S. Guo, and A. Y. Zomaya, "Distributed Segment-Based Anomaly Detection With KullbackLeibler Divergence in Wireless Sensor Networks," *IEEE Transactions on Information Forensics and Security*, vol. 12, no. 1, pp. 101–110, 2017.

[11] D. Oh, D. Kim, and W. Ro, "A malicious pattern detection engine for embedded security systems in the internet of things," *Sensors*, vol. 14, no. 12, pp. 24 188–24 211, 2014.

[12] S. Raza, L. Wallgren, and T. Voigt, "SVELTE: Real-time intrusion detection in the Internet of Things," *Ad hoc networks*, vol. 11, no. 8, pp. 2661–2674, 2013.

[13] D. Shreenivas, S. Raza, and T. Voigt, "Intrusion detection in the rpl-connected 6lowpan networks," in *Proceedings of the 3rd ACM International Workshop on IoT Privacy, Trust, and Security*. ACM, 2017, pp. 31–38.

[14] A. Le, J. Loo, K. Chai, and M. Aiash, "A specification-based ids for detecting attacks on rpl-based network topology," *Information*, vol. 7, no. 2, p. 25, 2016.

[15] E. Asgeirsson and C. Stein, "Vertex cover approximations on random graphs," in *International Workshop on Experimental and Efficient Algorithms*. Springer, 2007, pp. 285–296.

[16] A. Dunkels, B. Gronvall, and T. Voigt, "Contiki-a lightweight and flexible operating system for tiny networked sensors," in *Local Computer Networks, 2004. 29th Annual IEEE International Conference on*. IEEE, 2004, pp. 455–462.

[17] F. Osterlind, A. Dunkels, J. Eriksson, N. Finne, and T. Voigt, "Cross-level sensor network simulation with cooja," in *Local computer networks, proceedings 2006 31st IEEE conference on*. IEEE, 2006, pp. 641–648.

[18] M. Al Qurashi, C. M. Angelopoulos, and V. Katos, "Efficient intrusion detection in ad-hoc networks," in *6th International Symposium for ICS & SCADA Cyber Security Research 2019 6*, 2019, pp. 117–125.