Smart Attacks on the integrity of the Internet of Things: Avoiding detection by employing Game Theory

George Margelis*, Robert Piechocki*, Theo Tryfonas*, Paul Thomas†
*Communication Systems and Networks Research Group
MVB, School of Engineering
University of Bristol, UK
†University of Bristol Honorary Research Fellow
george.margelis@bristol.ac.uk

***Abstract*—The Internet of Things (IoT) is expected to connect billions of devices, that will interact with their physical environment through sensors or actuators. The measurements created from these sensors have varying levels of precision, leading to measurements that follow a distribution, whose variance presents an additional challenge for the employed security schemes.**

In this work we assume a smart attacker would attempt to mask his attack in the inherent uncertainty of the measurements, and attempt to manipulate the distribution of measurements as covertly as possible to affect the final meaningful value that the system would result in. We employ Game Theory to examine the best strategies to slowly corrupt the integrity of an IoT network, similar to ETSI's Low Throughput Networks (LTN). We examine the extent of the changes that can be made to the distribution without assuming a priori knowledge of it by the attacker, for different scenarios and compromisation patterns. To the best of our knowledge this is the first attempt to examine the limits of the compromise that could be applied by a smart attacker on an IoT/LTN-type network without triggering outlier-alarms, and can be applied in the design of better targeted defensive measures.

I. Introduction

In the vision of an IoT, physical objects have virtual representations, they can be controlled remotely and they act as physical access points to internet services[1]. Thus the physical world can be controlled through the virtual one. However, this introduces new risks as attackers can potentially gain access to systems considered so far secure. In addition, the protocol homogeneity needed for such a network is currently still missing. Currently, the field is fraught with competing solutions, based either on open or proprietary standards. This shifting environment makes designing system-wide security measures significantly harder as vulnerabilities in one protocol can act as entry-points to more tightly-secured components of the network.

Furthermore, in the IoT, the majority of the nodes will be deployed in locations where they can be exposed to various external factors, malicious or not. These nodes will be fitted with sensors with limited precision, to reduce costs, thus leading to measurements having not one precise value but rather a distribution of values. Because of the uncertainty inherent in the measurements, identifying when a node is malicious or simply malfunctioning is complicated. Similarly complicated is the process of deciding if a group of nodes are communicating values that deviate from the mean because they are compromised or simply because they are the first group to sense a change in the measured values. In the IoT uncertainty is embedded in the system.

An intelligent attacker would take all of the above into account when trying to penetrate an IoT-like network. Thus, understanding how an attacker would approach the penetration of the network, is crucial to develop security measures at the design phase instead of implementing them afterwards (what is traditionally known as bolt-on security, often not robust enough [2][3]).

In this paper we examine the strategies available to an attacker who attempts to compromise an IoT type network similar to LTNs that are currently on the rise [4] [5]. We apply game theory to explore the upper limits of the actions that an attacker can exert on the network before he is detected, including compromising nodes, changing the reported value of those nodes and assessing the feasibility of shifting the distribution of the reported measurements to a false value without being detected.

The structure of the paper is as follows: Section II discusses related works in intrusion detection for an IoT-like network. Section III defines our threat model while Section IV presents the principles of Game Theory that we apply in our work and our model. Finally, Section V contains our results and a discussion of them and section VI offers our conclusions.

II. Related work

Extensive work has been done in the past in the field of outlier detection and intrusion detection schemes as a way to identify malicious nodes in Wireless Sensor Networks (WSN). In [6] a scheme was proposed where the cluster head collects information from each node such as the node's ID or number of retransmissions per packet to identify possible anomalies. However, the incurred overhead can significantly reduce the battery life of the nodes. In [7] a system based on Machine Learning is employed to identify sampled packets as malicious

or not, depending on the feedback of the enviroment with high detection rate and low energy consumption for WSNs. More recent works in the field that employ outlier detection of malicious nodes can be found in [8] and[9].

However, schemes as the previously mentioned do not take into account modern penetration strategies, that tend to compromised a large number of nodes first before changing their behaviour [10]. Modern botnets tent to remain inactive until a sufficient number of nodes have been compromised and then they launch an attack. Furthermore, outlier detection can lead to false positives in a scenario where the majority of the nodes have been compromised, as the outliers will be the uncompromised nodes.

The question of how compromising a number of nodes in a sensor network would affect the overall system has been explored in [11] recently. The authors examine the effect of attacking sensors in a group to the overall distribution of measurements, however, they assume that the attacker has access to the measurements of all sensors, which effectively means that the attacker has already compromised the network. In contrast, in our work the attacker has access only to the data of the compromised nodes, a much more realistic scenario.

III. Defining a Smart Attacker

When discussing the security services of a system, assumptions are often made regarding the attacker that narrows the thread models to the ones that can be dealt by the defender i.e. the behaviour of the attacker is assumed to fit a pattern that is not necessarily the worst possible for the defender. Consider the case of a Jammer [12] for example: Security measures have been proposed to safeguard systems against jamming, however, they often assume that the Jammer transmits constantly in the same frequency,something very energy-inefficient. Fewer works examine the possibility of an reactive Jammer [13] that listens for transmissions before jamming and thus is both harder to detect and more efficient.

The aim of this work is to examine strategies that an intelligent attacker would use. We assume that the highest priority of this attacker is to avoid detection first, and then perform a system-wide data integrity attack. Here a data integrity attack is defined as a type of attack that aims to mislead the system in such a way as to achieve the goal of the attackers on a system level.

We assume then, that the attacker has the ability to compromise nodes, but understands that changing the behaviour of a node too radically would be identified by systems employing outlier detection techniques [14] [15]. This behaviour has already been observed in the wild, with most prominent example being Stuxnet [16], [17]. Stuxnet introduced a new kind of attack model, where the attacker infects nodes of the network and propagates without disturbing the network until a specific condition has been met. The malware then minimally changes the behaviour of some nodes in some way, enough to disturb the integrity of the network but not enough to trigger outlier alarms. We also assume that the attacker, due to the aforementioned, tries to conceal the compromised nodes in the inherent measurement uncertainty of an IoT network that spans hundreds or thousands of nodes.

In practical scenarios, even uncompromised distributions that should be normal tend to be slightly skewed due to environmental or other non-malicious reasons like node malfunction. Thus, comparisons must take into account that there is a margin for error that does not necessarily identify an attack but rather the practical realities of an IoT system. It is this margin of error that an intelligent attacker would exploit to hide. As a result, the extend that the attacker can shift the uncompromised distribution is limited by this uncertainty, as certain shifts might require behaviour that would make the attack easily identifiable. In this work we aim to assess this limit and the best strategies to reach it.

IV. Applying Game theory

Game Theory has been used extensively in the past for modelling and solving security related problems in networks [18][19][20] as it allows us to abstract the network vulnerabilities and develop general security strategies. A game in normal form is a tuple $G = \langle N, A, u \rangle$ where:

- $N = \{1, 2, ..., n\}$ a set of n rational players indexed by i. By rational in this context we mean that the player chooses the strategy that maximizes his payoff when being able to calculate the results of every action.
- $A = A_1 \times \ldots \times A_n$, where A_i is a finite set of actions available to player i. Each vector $a = (a_1, \ldots, a_n) \in A$ is an action profile.
- $u = (u_1, \ldots, u_n)$ where $u_i : A \to \mathbb{R}$, is a real valued payoff function for player i.

The attacker, being rational, ideally follows the minmax strategy, that is the strategy that guarantees a minimum payout for him no matter the choice of his adversary, instead of another strategy that can lead to higher payouts in some cases but losses in others:

$$u_i = \min_{a_i} \max_{a_{-i}} u_i(a_i.a_{-i})$$

Where i is the index of the attacker, $-i$ is the index of other players except the attacker, a_i is the action taken by player i and a_{-i} the actions taken by all other players. A minimum payout of course in this case means that he indeed manages to shift the distribution by avoiding detection no matter how strict the threshold is set by the defender. In our game, being zero-sum, the minmax strategy is the same as the strategy of the Nash Equilibrium which informally can be understood as a strategy that the attacker would not want to deviate from, if he knew what strategies the defender was employing.

A. Proposed Model

We are interested in modelling a network that behaves similarly to Low Throughput Networks (LTN) that are starting to become more popular for certain applications. These include LoRaWAN or Sigfox networks. The networks have a star topology, and the nodes communicate a measured value in either scheduled or opportunistic manner. The basestation can

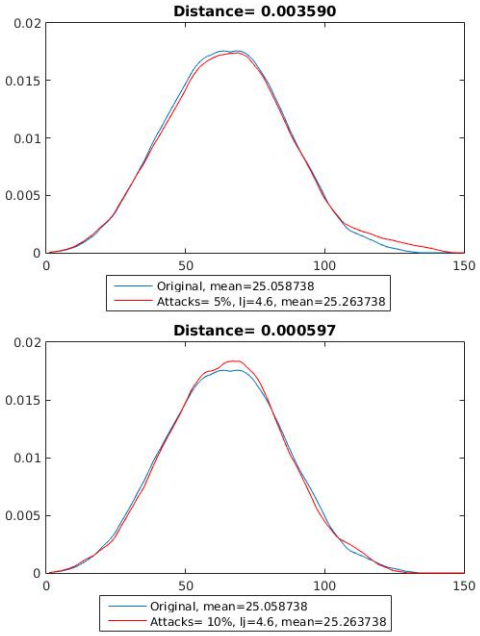

Figure 1: The effects of different strategies in the shape of the distribution. In both cases the mean of the distribution has been shifted by 0.2 but the distance of the resulting distribution is much higher in the case of the fewer compromised nodes.

then use these values to derive the mean value which is the one that is reported back to the user(s).For an example of a system that exhibits such behaviour refer to [21].

We expect the measurements to follow a normal distribution with standard deviation that depends on the quality of the components, and covariance zero: Cheaper components would lead to a bigger standard deviation as measurements would deviate more but measurements that come from different components will be independent of each other. This in effect models a system that has been deployed for environmental monitoring, where the nodes have been deployed in an area and measure a variable like humidity or acidity.

At a given time, the attacker wishes to move the mean of the uncompromised distribution towards a value of his choosing. The attacker earns the reward if he manages to move the mean to the one of his choosing but pays a penalty that is a function of the number of compromised nodes. The dilemma that the attacker faces is if it is better to attempt to compromise more nodes at a bigger cost and shift their reported value to a lesser extend, or compromise less nodes and shift their reported value more radically increasing the chance of detection. An example can be seen in figure 1.

The defender earns the reward when she detects that an intrusion is taking place. Because she does not know how many nodes have been compromised she checks the shape of the distribution of received values and compares it with an accepted shape (the accepted shape can be the result of training).

When attempting to compare two distributions it is intergral to define how that comparison takes place and which metrics are used to measure the distance of the two. For a more elaborate discussion on the suitability of certain distance metrics, refer to [22]. We should briefly mention that we examined using both the Euclidean distance and the Kullback-Leibler divergence as metrics. However both are overly sensitive to inequalities of support of the two distributions. Therefore we employ Hellinger's distance, a type of f-divergence. f-divergences were introduced by Csiszár in 1963 and are extensively used as measures of similarity and orthogonality between distributions. A full description of their properties is out of the scope of this paper but for more information refer to [23]. Hellinger's distance is defined as

$$D_H(p,q) = -ln\left(\sum_x \sqrt{p(x)q(x)}\right)$$

where $p(x)$ is the uncompromised distribution and $q(x)$ is the compromised. We have chosen to use this metric as it allows us to make the least number of assumptions regarding the compared distributions. It is less sensitive than the previously mentioned to inequalities in the support of the distributions, which can emerge even under normal circumstances.

We make the following assumptions

- Our system reports a value that is the mean of the distribution of the values the network of nodes communicate to the basestation.
- The attacker can see the final reported value.
- Every attack that the attacker attempts is successful, leading to a compromised node.
- The attacker attempts to change that reported value to something else, which we name *"Attacker's Target"*.
- The attacker controls the number of compromised nodes (A) and how much the value of the compromised nodes differs compared to the value that the node would report if it wasn't compromised (l_j).
- The attacker does not know the value that the uncompromised nodes communicate to the base station.
- The defender does not know how many nodes have been compromised.
- The defender knows all the values that the sensor network reports.
- Both the attacker and the defender are rational.
- The choices of the players are independent, which models that the choices are not coordinated.

When an attack takes place there are only two possible outcomes for the attacker: He is either detected, or he succeeds in compromising the network. This can be modelled as a zero-sum game. The utility function of this game is the following:

$$\begin{aligned} AP = (\mu \geq AT) \cdot (\text{RWD}) - A \cdot (\text{CPA}) \\ - (D_{(p,q)} > \text{Threshold}) \cdot 2 \cdot (\text{RWD}) \end{aligned} \quad (1)$$

where AT is the *"Attacker's Target"*, RWD is the reward for compromising the network or detecting the attack, A the number of compromised nodes, CPA the cost per attack that

leads to a node being compromised and $D_{(p,q)}$ the Hellinger distance of the distributions. As detection of the attack leads to an immediate loss for the attacker, the RWD for the defender is doubled. Moreover,:

$$\mu = \frac{\sum_{i=1}^{N-A} x_i + \sum_{j=1}^{A}(x_j + l_j)}{\sum_{i=1}^{N} x_i}$$

where N the number of deployed nodes, x_i the value node i would report if it was not compromised and l_j the difference between x_j and the value the compromised node is reporting. Furthermore,:

$$(\mu \geq AT) = \begin{cases} 1, & \text{if inequality holds} \\ 0, & \text{otherwise} \end{cases}$$

and similarly

$$(D_{(p,q)} > \text{Threshold}) = \begin{cases} 1, & \text{if inequality holds} \\ 0, & \text{otherwise} \end{cases}$$

Threshold is the upper boundary that our system will accept a distribution as uncompromised. The pseudo-code for our model is:

for N number of nodes
Generate K
end for
for $a \in \{1, 2.., N\}$
for $l_j \in \{\mu/250, 2\mu/250, ...\mu/5\}$
Create $Compromised\_Distribution_{(a,l_j)}$
Calculate μ
end for
end for
for $T \in \{T_{min}, T_{max}\}$
Calculate $D_{(p,q)}$ *for K*
Populate $PM_{(T)}$ *according to equation (1)*
$NashEq_{(T)} = ne(PM_{(T)})$
end for
Find strategies lead to NashEq $\forall(PM_{(T)})$

Where K a normal distribution of identically distributed but not independent values for the N nodes, T the threshold of the distance metric and PM the respective payout matrix.

V. Results and Discussion

We examine three different scenarios that model different types of compromise.Due to space considerations a subset of the payout matrices are visualised with contour maps to facilitate inspection. For each scenario we present how the feasibility of the attacks change as the attack target gets higher. For brevity we only illustrate for each scenario the results for three different attack targets, that is for a shift of the mean value by 1%, 5% and 8% although our numerical results reach up to attack targets of 20%. The progression of the cost for every scenario can be seen in figure 2.

A. Scenario 1: Cost of attacks remain constant

For the first scenario we assume that the cost that the attacker pays to compromise a node (whether that is measured in resources or something else is not important) remains constant over time

We examine first the case where the attacker aims to shift the mean by 1%; a subset of the results can be seen in figure 3. Each plot represents the payout matrix, where deep red implies a win for the attacker and other colours a failure for the attacker. In all related figures to follow, the Nash Equilibrium is denoted by a white dot.

From our results, we can see that for modest attack targets it is possible for the attacker to shift the distribution and avoid being detected. When the attacker's target is to shift the mean by 1% there is a Nash Equilibrium strategy that leads to a successful compromise with 5.2% of the nodes compromised. As can be expected when facing more strict defenders, a larger number of nodes must be compromised.

As the attacker becomes more ambitious the percentage of nodes that must be compromised to retain the expected shape of the distribution becomes significantly higher. For a shift of 5% of the mean the attacker needs to compromise 94% of the nodes for strict defenders but for more relaxed cases, the objective can be achieved by compromising 25.6% of the nodes. Shifting the mean by 8% can be achieved by attacking 41% of the nodes, though for stricter thresholds up to 94% of the nodes must be compromised.

A summary of our results can be seen in figure 4 where we can see as the relationship between the threshold and the minimum number of nodes needed to be compromised for the attacker to achieve his objective. From figure 4, the attacker can choose his strategy if he has an estimation of the threshold employed by the defender.

B. Scenario 2: Cost of attacks rises over time

The second scenario assumes that cost of the attacks increases over time. This models that, the possibility of being detected increases as time passes and transforms the game into a discounted game, in game theoretical terms. The results of

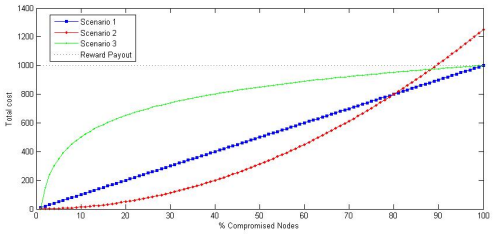

Figure 2: Cost for the attacker as number of compromised nodes increases for our scenarios.

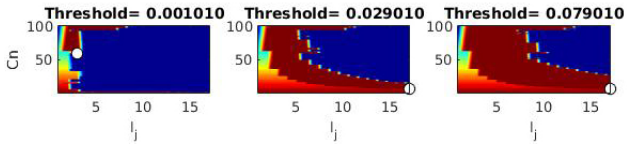

Figure 3: Payout for the attacker for the first scenario when the attacker aims to shift the mean of the distribution 1% higher.

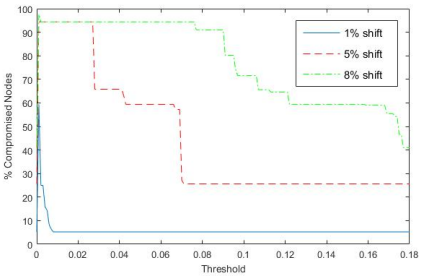

Figure 4: Percentage of Nodes needed to be compromised vs. Threshold for the attacker to win the first scenario.

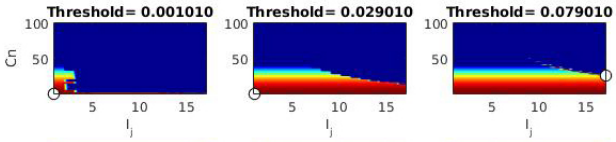

Figure 5: Payout for the attacker for the second scenario when the attacker aims to shift the mean of the distribution 5% higher.

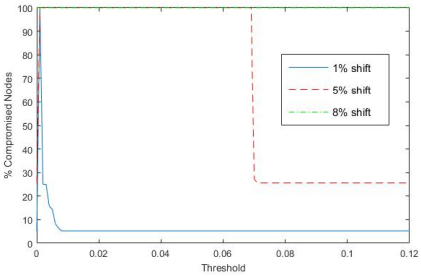

Figure 6: Percentage of Nodes needed to be compromised vs. Threshold for the discounted game.

our model for this scenario are partially illustrated in figure 5. We can see that the attacker can achieve his objective just by compromising 5.2% of the nodes when the aim is to shift the mean just by 1%. That is due to the lower cost compared with scenario 1 of the initial attacks. A shift of 5% is possible when compromising 25.6% of the nodes.

However, there is an upper boundary on how much can an attacker shift the mean, and that is 8%. From that point on,the total of the deployed nodes need to be compromised. We should also point here that when the attacker needs to compromise 100% of the nodes to achieve his objective, his payout is penalized by an amount equal to the reward (or even higher as in the case of the second scenario). Thus the nature of the game is such that the Nash equilibrium is found at the lowest row of the matrix, that is at 0% compromised nodes, where he has not earned the reward but there is zero cost also. Understanding this may seem trivial, but it is important to explain the results in figures 5 and 7.

C. Scenario 3: Cost of attacks lowers over time

The third scenario assumes that the ease of the attacks is low at first but increases as more nodes become compromised, having the inverse effect on the cost.This scenario models cases where vulnerabilities allow attacks to propagate in a way

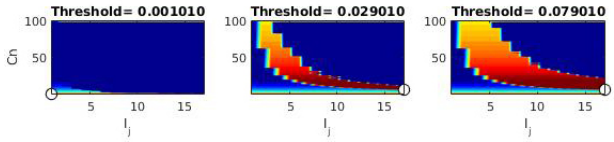

Figure 7: Payout for the attacker for the third scenario when the attacker aims to shift the mean of the distribution 1% higher.

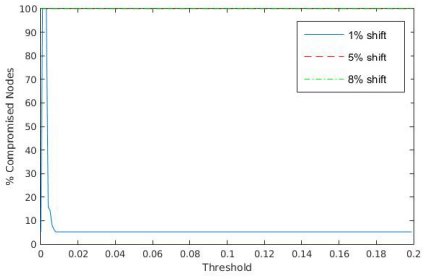

Figure 8: Percentage of Nodes needed to be compromised vs. Threshold for the third scenario.

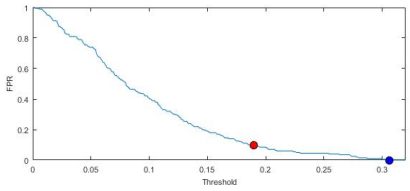

Figure 9: FPR vs Threshold.The blue marker denotes the point where the FPR becomes 0, while the red the point where the FPR becomes 10%.

similar to the one active worms spread, as described in [24].

Once again, it is possible for the attacker to achieve his objective. However, the high initial cost hinders the attackers attempts and requires a more relaxed threshold for him to succeed. We can derive from this that from the defender's perspective, this is the best outcome. This provides some insight to the question faced often when designing a network regarding its security schemes: Should devices be protected individually or in groups? The results of scenario 3 hint that individual protection (which is modelled by the high initial cost for the attacker) can lead to better results, although in vast deployments it might be impractical to ensure robust protection for all nodes.

D. Threshold and False Positives Rate

A common result in the above scenarios is that as the threshold increases, the attacker needs to compromise less nodes to achieve his objection. One might wonder what is a reasonable value for the threshold then and what is the False Positive Rate (FPR) that emerges in relationship with the value of the threshold. We can see the numerical results of that exploration in figure 9. In this study, we define FPR as FPR=FP/(FP+TN) where FP is number of false positives, and TN is number of true negatives.

Threshold	FPR	Scenario 1 Attacker's Target			Scenario 2 Attacker's Target			Scenario 3 Attacker's Target		
		1%	5%	8%	1%	5%	8%	1%	5%	8%
0.02	74%	5.2%	94.4%	94.4%	5.2%	100%	100%	5.2%	100%	100%
0.1	40%	5.2%	25.6%	71.6%	5.2%	25.6%	100%	5.2%	100%	100%
0.2	7%	5.2%	25.6%	41%	5.2%	25.6%	100%	5.2%	100%	100%

Table I: Minimum percentage of compromised nodes needed for the attacker to win per scenario and target.

Our simulations show that a system that examines the shape of the distribution as a security measure would need to set the threshold as high as 0.19 to keep FPR as low as 10% and at least 0.306 to eliminate any FP. A summary of the effects of Threshold to FPR and the percent of compromised nodes that the attacker needs to compromise to win can be seen in table I.

VI. Conclusions

In this work we examined how an intelligent attacker would proceed to compromise the integrity of a network by attacking nodes of the network and moderately changing the value they report to the basestation. This leads to a shifting of the distribution of measurements and eventually to an attack of the integrity of the network. We employed Game Theory to model our network and the attacks in an abstract way and avoid reaching conclusions that are applicable only to specific protocols and technologies.

We studied three different scenarios regarding the cost that the attacker pays to compromise nodes. In all of the cases it was clear that the attacker can achieve modest shift targets, even for strict thresholds. Furthermore, for systems that employ a more lax threshold to avoid false positives the attacker can achieve even more ambitious objectives like shifting the mean of a distribution by 8%.

Our work can be extended to aid the design of security measures of a network, by employing risk analysis to techniques to correctly model the cost function that mirrors the characteristics of designed network. The aforementioned scenarios model specific cases, however many more can be explored.

Acknowledgment

This work was supported by the Engineering and Physical Sciences Research Council [EP/I028153/1] and the University of Bristol.

References

[1] F. Mattern and C. Floerkemeier, "From the internet of computers to the internet of things," in *From active data management to event-based systems and more*. Springer, 2010, pp. 242–259.

[2] K. S. Wilson and M. A. Kiy, "Some fundamental cybersecurity concepts," *Access, IEEE*, vol. 2, pp. 116–124, 2014.

[3] K. Fu and J. Blum, "Controlling for cybersecurity risks of medical device software," *Communications of the ACM*, vol. 56, no. 10, pp. 35–37, 2013.

[4] G. Margelis, D. Kaleshi, R. J. Piechocki, and P. Thomas, "Low throughput networks for the IoT: lessons learned from industrial implementations," in *2015 IEEE World Forum on Internet of Things (WF-IoT) (WF-IoT 2015)*, Milano, Italy, Dec. 2015.

[5] C. Goursaud and J. M. Gorce, "Dedicated networks for iot: Phy / mac state of the art and challenges," *EAI Endorsed Transactions on Internet of Things*, vol. 15, no. 1, 10 2015.

[6] S. Gupta, R. Zheng, and A. M. Cheng, "Andes: an anomaly detection system for wireless sensor networks," in *Mobile Adhoc and Sensor Systems, 2007. MASS 2007. IEEE International Conference on*. IEEE, 2007, pp. 1–9.

[7] S. Misra, P. V. Krishna, and K. I. Abraham, "A simple learning automata-based solution for intrusion detection in wireless sensor networks," *Wireless Communications and Mobile Computing*, vol. 11, no. 3, pp. 426–441, 2011.

[8] V. P. Illiano and E. C. Lupu, "Detecting malicious data injections in wireless sensor networks: a survey," *ACM Computing Surveys (CSUR)*, vol. 48, no. 2, p. 24, 2015.

[9] M. Salehi, C. Leckie, J. C. Bezdek, and T. Vaithianathan, "Local outlier detection for data streams in sensor networks: Revisiting the utility problem invited paper," in *Intelligent Sensors, Sensor Networks and Information Processing (ISSNIP), 2015 IEEE Tenth International Conference on*. IEEE, 2015, pp. 1–6.

[10] M. Abu Rajab, J. Zarfoss, F. Monrose, and A. Terzis, "A multifaceted approach to understanding the botnet phenomenon," in *Proceedings of the 6th ACM SIGCOMM conference on Internet measurement*. ACM, 2006, pp. 41–52.

[11] R. Yan, T. Xu, and M. Potkonjak, "Data integrity attacks and defenses for intel lab sensor network," in *2015 IEEE World Forum on Internet of Things (WF-IoT) (WF-IoT 2015)*, Milano, Italy, Dec. 2015.

[12] W. Xu, T. Wood, W. Trappe, and Y. Zhang, "Channel surfing and spatial retreats: defenses against wireless denial of service," in *Proceedings of the 3rd ACM workshop on Wireless security*. ACM, 2004, pp. 80–89.

[13] Y. Liu and P. Ning, "Bittrickle: Defending against broadband and high-power reactive jamming attacks," in *INFOCOM, 2012 Proceedings IEEE*. IEEE, 2012, pp. 909–917.

[14] E. M. Knorr, R. T. Ng, and V. Tucakov, "Distance-based outliers: algorithms and applications," *The VLDB Journal—The International Journal on Very Large Data Bases*, vol. 8, no. 3-4, pp. 237–253, 2000.

[15] Y. Zhang, N. Meratnia, and P. Havinga, "Outlier detection techniques for wireless sensor networks: A survey," *Communications Surveys & Tutorials, IEEE*, vol. 12, no. 2, pp. 159–170, 2010.

[16] N. Falliere, L. O. Murchu, and E. Chien, "W32. stuxnet dossier," *White paper, Symantec Corp., Security Response*, vol. 5, 2011.

[17] R. Langner, "Stuxnet: Dissecting a cyberwarfare weapon," *Security & Privacy, IEEE*, vol. 9, no. 3, pp. 49–51, 2011.

[18] Y. B. Reddy, "A game theory approach to detect malicious nodes in wireless sensor networks," in *Sensor Technologies and Applications, 2009. SENSORCOMM'09. Third International Conference on*. IEEE, 2009, pp. 462–468.

[19] M. Asadi, C. Zimmerman, and A. Agah, "A game-theoretic approach to security and power conservation in wireless sensor networks." *IJ Network Security*, vol. 15, no. 1, pp. 50–58, 2013.

[20] T. Spyridopoulos, G. Karanikas, T. Tryfonas, and G. Oikonomou, "A game theoretic defence framework against dos/ddos cyber attacks," *Computers & Security*, vol. 38, pp. 39–50, 2013.

[21] W. Mobile, "Real-time maps and traffic information based on the wisdom of the crowd," *Retrieved April*, vol. 7, p. 2011, 2010.

[22] J. Chung, P. Kannappan, C. Ng, and P. Sahoo, "Measures of distance between probability distributions," *Journal of mathematical analysis and applications*, vol. 138, no. 1, pp. 280–292, 1989.

[23] F. Österreicher, "Csiszár's f-divergences-basic properties," *RGMIA Res. Rep. Coll*, 2002.

[24] Z. Chen, L. Gao, and K. Kwiat, "Modeling the spread of active worms," in *INFOCOM 2003. Twenty-Second Annual Joint Conference of the IEEE Computer and Communications. IEEE Societies*, vol. 3. IEEE, 2003, pp. 1890–1900.