جامعة نايف العربية للعلوم الأمنية
Naif Arab University for Security Sciences

Naif Arab University for Security Sciences
Journal of Information Security & Cybercrimes Research
مجلة بحوث أمن المعلومات والجرائم السيبرانية
https://journals.nauss.edu.sa/index.php/JISCR

JISCR

Trust Modeling in Wireless Sensor Networks: State of the Art

Mohammed Mahdi Alqhatani*, Mostafa G. M. Mostafa
Department of Network Security, College of Computer and Information Security, Naif Arab University for Security Sciences, Riyadh, Saudi Arabia.

Received 01 Apr. 2018; Accepted 20 May 2018; Available Online 30 May 2018

Abstract

Wireless sensor networks (WSNs) is the backbone of the new generation of internet of things (IoT). WSNs are growing rapidly and security threats are increasingly growing as well. Trust computing plays a crucial role in WSN security modeling. In WSN node trust is important to keep the network safe and operational. This paper presents the state-of-the-art techniques in WSN Trust modeling. Comparison and analysis of most recent solutions were conducted. Direction and trends of current and future research approaches are also presented.

I. Introduction

Nowadays, it is not only necessary to implement trust model for boosting security in Wireless sensor networks (WSNs), but also it is crucial to analyze how to resist attacks with that trust scheme. Furthermore, in general, trust in WSNs can be classified into two broad categories, user trust and system trust. The notion of "user trust" is derived from psychology and sociology, with a standard definition as "a subjective expectation an entity has about another's future behavior". "System trust" is the expectation that a device or system will faithfully behave in a particular manner to fulfil its intended purpose". Trust relies on the integrity, ability and other characteristics of an entity [1].

Network security, generally, deals with confidentiality, integrity and availability, in WSNs, it should also consider revocation of suspicious elements. WSNs security aims to increase dependability of their mechanisms. It can be achieved by strengthening trust and privacy, as shown in Fig. 1. Security performs by employing reliable cryptographic methods, symmetric or asymmetric authentication approaches, meanwhile trust concerns about recommendation and reputation and so forth. It can be presented by various trusting establishment methods, such as, fuzzy logic, bio-inspired, machine learning or deterministic & probabilistic- based methodology. On the other hand, privacy can be established through agreements, laws and code of ethics. There are a specifics circumstances such as limited resources, harsh and un-attended environment in WSNs make building ideal system for all known threats even harder. No standard adversarial model where current trust security systems would compete to provide a higher level of security or resilience to attacks. Designers of such systems solved the trustworthiness problem in WSNs using various aspects; some designers considered only routing misbehaviours or task performance or ruggedness. Misbehaviour of nodes can affect the trust rating; therefore, it is Important

Keywords: *WSNs; Security; Privacy; Trust modeling; IoT.*

Production and hosting by NAUSS

* Corresponding Author: Mohammed Mahdi Alqhatani
Email: mmalsultan@gmail.com
doi: 10.26735/16587790.2018.007

to monitor such behaviours and control a trust level of the nodes. So, they will confidently rely on each other for further cooperation. To build a good trust model, reputation through sensor nodes is required to capture and prohibit the effect of intruders.

A socio-psychological based intelligent trust model for computing trust in WSNs was developed, which identifies three major components, namely, ability, benevolence and integrity. After computing the trust based on these components for each node in the WSN, an intelligence mechanism is utilized to remove malicious nodes with low trust to stabilize the network.

The aim of this paper is to present the state-of-the-art of trust modelling in WSNs. We presented and compared various mechanisms and investigated recent research direction in this context. This paper is organised as follows: Section II overview the WSNs. SectionIII attacks, countermeasures and obstacles in WSNs. Section IV present trust model in WSNs. Section VI Conclusion and Future Work.

II. WSNs Overview

WSNs is growing exponentially due to its utilization in various applications such as environmental monitoring, military applications, medical care units and health monitoring and so on. WSNs are networks of spatially distributed autonomous devices that can sense and monitor its environment. WSNs consist of many tiny, inexpensive, disposable and autonomous sensor nodes that are in small or huge geographical areas for remote operations. However, WSNs faces many challenges, mainly, computational limitation due to sensor resource constraints, e.g. storage, communication bandwidth and power supply. Security is also a big challenge that face WSNs. Moreover, trust between nodes within WSNs is emerging as a crucial factor in WSNs security systems. It has been increasingly studied by many researchers and remains an open and research gaps.

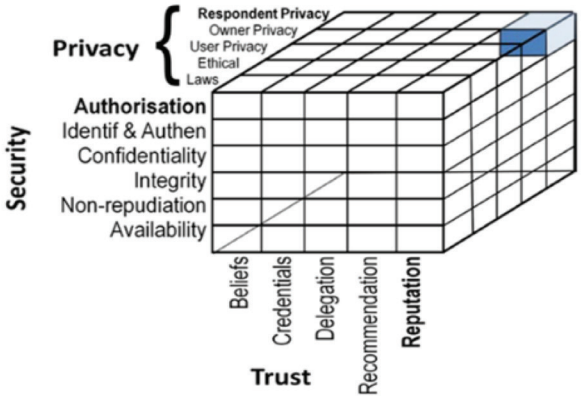

Fig. 1. WSNs Security, Trust and Privacy relationship. [ITU-T Technical Report: Standardization of Trust Provisioning Study (2015-12)] [2].

WSNs are recognized as a set of tiny low-cost devices called sensor nodes. Its small in weight, low cost of the hardware and ease of deployment of such platforms. By spatially distributing huge of such autonomous devices. After their deployment, sensors deliver their sensed data to back to dedicated nodes called sink nodes or base station. According to the used structure, the sink is reachable using wireless transmissions links such as Bluetooth, WIFI, 4G etc.

The research trends related to WSNs are many[3], e.g. development of models and improvement existing tools for the design of better WSNs architecture and design of standard protocols in WSNs to work robustly on scenarios. The factors influencing sensor network design is highly important to be fully integrated of all factors that are driving the design of sensor networks and sensor node simultaneously. These factors work as a guideline to design related protocols, algorithm or approach i.e. reliability, scalability, robustness, complexity either time or space etc.

In communication networks, protocols control and determine activity specifications how networks fulfil their intended use[4]. The sensor network protocol stack is same the traditional network protocol stack. With the layers of application, transport, network, data link, and physical. Frequency selection and generation are a mission of physical layer as well as data encryption and modulations process. Data link layer is responsible for the multiplexing of data packets. The network layer takes care of routing task. The transport layer helps to maintain the data flow and its important when network connected to internet as in Internet of Thigs (IoT) technology. Different types of application software can be used on the application layer according to the network tasks. A common plane shared above layers aims to optimize a management purpose, a different research been conduct-

ed in this context. The aims of security in WSNs is to protect the information and resources from external offensive, includes to ensures that certain network activity is available, authorization to approve that only authorized sensors generate information to the network, authentication which monitor the communication from one sensor to another is real, confidentiality which approve that a given data encrypted. Integrity which check that a message sent from one sensor to another is not change by any intermediate sensors. Forward and backward secrecy when a sensor should not be able to read any future messages after it leaves the network or when a joining sensor should not be able to read any previously message. Nonrepudiation means that a node can't refuse sending an information it has been sent previously. Finally, freshness implies that the data is recent and guarantee that adversary cannot replay old messages

III. Attacks and Countermeasures in WSN's

In this paper we classify the attacks in five categories upon their acts. In the following subsections, we will explain some of the well-known type of attacks and their countermeasure.

A. Attacks Injectting Packets in WSN

Vampire Attack: or some of them call it energy drain attack. Network layer is targeted by this attack, to disable WSNs by exhausted nodes' battery power. Most of examined routing protocol are subject of this type of attack by expose their vulnerabilities[5, 6]. The existing secure extension protocol aims to isolate adversary from discover routing path, while this attack can use the valid routing path. Author in [7], have present the mechanism that overcome the issue in AODV protocol, according to the coordinates of the attacker, the power consumed very fast through the forwarding phase, verifying that packets consistently make good progress.

Hello Flood Attack: Many protocols require node to broadcast HELLO messages to announce themselves to their neighbors. a message will assume one-hop communication to neighbor. Attacker utilize large transmission power to broadcast its HELLO message to cover a wide range of sensors. The receiving nodes will be thinking that the attacker is their one-hop neighbor[8]. one intuitive defense against such an attack is to verify the bi-directionality of a link between two "neighboring" nodes using LEAP protocol in this context.

Misdirection attack: the attacker aims to increase latency which lead the loss of actual packets, or direct the packet to go to compromised node instead of the true receiving node[9]. When the network management monitor such that behaviour, the mitigation process is to forces the compromised node to sleep mode for some time.

Flooding attack: in transport layer, attacker continually attempts to create new connection requests to exhausting recourses or reach maximum limit of iteration. To mitigate this issue, node must guarantee to the connection and demonstrate their faithfully. And set limit on the number of connections from a legitimate node[10].

B. Attacks Causing Noises in WSN

Jamming attack: shared medium of WSNs makes easy for adversaries to conduct radio interference, attacker impacts network operation by broadcasting high-power signals. There are many effective type of jamming, according to the purpose that attacks need to achieve[11]. The most important stage in detected and digenesis that the jamming is occur or still under that situation. It is challenging stage once involves discriminating between legitimate and fraudulent causes of week connectivity. frequency hopping modulation. Is a proper known technique in physical layer to continues carrier operation frequency to mitigate such this attack as well as game theory as described in [12].

Collision attack: mainly occur in MAC layer. send short noise message at same time that assigned for another node to send[10, 13]. In below example depicts of a scenario that happens in IEEE 8.2.15.4 where the contention access period using the MAC protocol, the authorized node sends a packet contain direction and length to guarantee time slot GTS, If the transceiver accepts the GTS, it will send a message to all nodes. At that time, the eavesdropper will know the location of GTS, already defined by extracting the GTS descriptor from the received beacon frame. After that, the interference can start and cause such attack of the GTS data packets between the authorized nodes and transceiver as shown in [14, Fig. 2].

carrier sense multiple access (CSMA) technique is one of proper technique utilized to mitigates the probability of collisions attack occurrence.

Black Hole attack: some of them call it sink hole attack, its network layer routing alteration with aims of attracting all the packets to compromised node, and silently discarding them to avoid triggering the route maintenance mechanism at a source node to select another route[15], [16]. A solution to defend against attack the following mechanisms are utilized [17]:

1. ***Source routing:*** the sender defines the sequence of nodes that has to passthrough till destination.
2. ***Destination acknowledgments:*** acknowledgment signals send it back to the sender in same route and reverse direction
3. ***Timeouts:*** the sender and nodes in between set a time to each packet data for expecting acknowledgment signal passthrough or raised fault indication from other nodes in between.

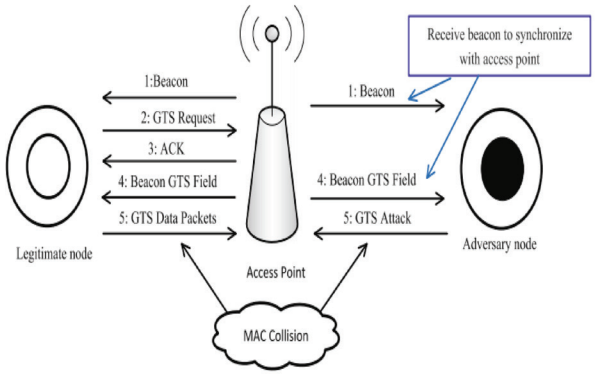

Fig. 2. Collision Attack [14].

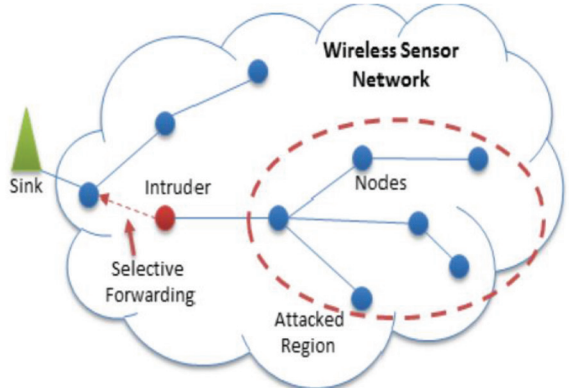

Fig. 3. Selective Forwarding Attack [21].

4. ***Fault announcements:*** if the signal timer is time-out, indication alarm send to the source.

Denial of Service (DoS) attack: attacker deception sensor nodes by flooding a multi hop end-to-end communication path with either replicated packets or spurious injected packets. This attack has many forms and can describe in this section in different subsection i.e. jamming, hello floods, spoofing, replaying, or altering routing. The attack can tend noise generation at different layers function[11], [18].

Selective Forwarding attack: or some of them call it Gray Hole attack. The attacker tend to stop the packets in the network by either rejecting to forward or alter passing through them [19], [20] .

To mitigate, there are couple of techniques that using acknowledgement, neighboring node's information or techniques that use multiple data flow paths that eliminates attack's effects [21, Fig. 3].

For all types that briefed in subsection B, the detect and defend spam scheme (DADS) proposes a concept of quarantine regions to "isolate" spam attackers, In DADS, the far-end sink is looking after checking whether there are spam attacks in the network. The far-end sink can monitor the packets as follows [22]:

1. Analyses and filter the node send a faulty signal frequently.
2. Utilize the frequencies of messages sent by the sensor nodes in the same region.
3. Count the packet rate of the overall sensor network.

C. Attacks Injectting Packets and causing Noises in WSN

Spoofed attack: eavesdropper Impersonates another node identity [23]. Countermeasure of such attack, can be through signature verification method as one of techniques that identify the attackers and prevented them through which the data is transferred through the correct node.

Sybil attack: Many node identities forges their identity [24], [25]. Attack aim the integrity of the traffic, it works against the algorithm that attempts to enhance resource consumption. This attack could be prevented using efficient protocols. However, detection of such Sybil nodes in a network is not so easy. radio resource

testing based on the assumption that each physical node (including the attacker) has only one radio and cannot simultaneously send or receive on more than one channel so, a node assigns each of its neighbors a different channel to broadcast messages, then the node then randomly selects a channel to listen. Another scheme to defend against such attack is random key pre-distribution, which is derived from the key pool scheme, where randomly assigns k keys to each node from a pool of m keys. If two nodes share q common keys, they can establish a secure link. The random key pre-distribution scheme solves this problem using a pseudo-random hash function to assign keys and validate the identity of a node.

Wormhole attack: is consists of two nodes. The attacker nodes that are connected by a high-power and low latency link known as the tunnel[26]. Wormholes can create a fake network topology by relaying packets between two distant nodes. In this case, these two distant nodes may be considered as neighbors of each other. The concept of packet leash is introduced to defend against such attacks [27]. A leash is the information added in a packet to restrict the packet's maximum allowed transmission distance.

D. Attacks on applications in WSN

Application attacks: in this layer many couple of known attack i.e. overwhelm attack, as target bandwidth consumption, data corruption attack. Generally, attack modifies the firmware/software that is stored in a node [28]. Risk management process and updated the operating system software are the mechanisms that tend to mitigate the threats.

In Summary, we had been discussed the most known attacks and categories them as Fig. 4 upon the function of the attack.

IV. Trust Models in Wireless Sensor Networks

Trust has common attributes in different networks. its subjective and this provided by some observers or recommender, depending on certain records of past behaviour. its dynamic and may change over time and space. its asymmetric since its mutually independent between both sides, that is to say, A trusts B while B may distrust A. its incomplete transitive by means the trust link exists, but

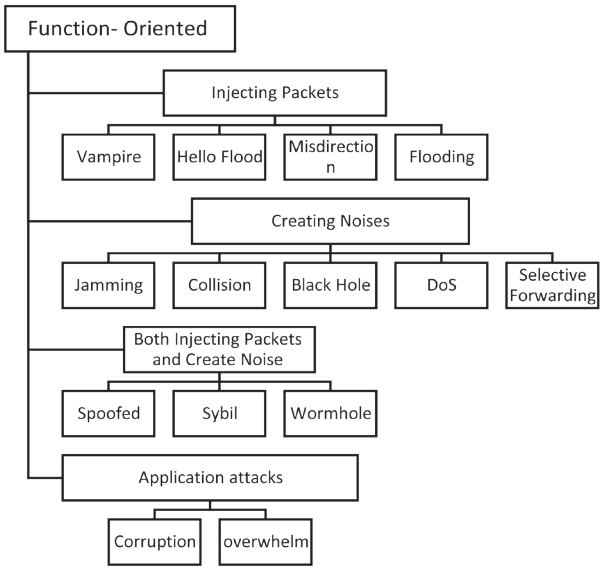

Fig. 4. Attacks Category as Function Oriented.

depending on the structure or extent of the trust relationships among participants, A trust B, and B trust C, while A may trust or distrust C.

A. Schemes Classified Based on Their Application and Services

Node-Based trust models: when we look to previous trust models studies we can observed that has two types of models, first one takes one location to do the process of trusting in the network that is called centralized models, the other type is leave the process of trusting distributed over the sensors, so each sensor must do their computation for their trusting of neighbor sensors, those type of models called distributed models or flat structure models. In [29], TMM based on D–S theory proposed a model to solve the problem of quantification and uncertainty of trust, it has advantages over the oldest models in context in classifying the malicious node behaviour and present good in scalability. In [30], proposed two modules for key building, the first one called watchdog, and their task is to monitor actions of neighbor sensors as well as classify that actions to cooperative or not. The second module is called reputation system to control the sensor reputational. It was assuming the module has enough process and interactions between sensors to give ability of the model to reach the stationary state. The reputational module will not work effectively if the sensors

TABLE I
NODE-BASED TRUST MODELS COMPARISONS

	Scheme	characteristics	Prons	Cons	Features that addressed
Node-Based trust models	TMM based on D–S theory[29]	Relation of temporal and spatial data, by sensor nodes in adjacent area. Calculate the number of interactive behavior of trust, distrust or uncertainty. flexible method is adopted to calculate the overall trust.	Solve the problem of quantification and uncertainty of trust.	Subject to enhance performance of model.	authentication of user
	RFSN[30]	Reputation-based Framework for Sensor Networks based on probability theory and Bayesian network; Using Watchdog to monitor neighbour nodes' actions.	Trust computation is precise without single point failure.	Can improve security of each node, but cannot improve system robustness. Bayesian calculation requires memory and computational complexity. if node move reputation not stabilize. only propagate good reputation for another node.	Collision attack and On-Off attack.
	NBBTE[33]	Model proposed based on behavior strategy banding D–S belief theory, Weighting; Fuzzy theory and D–S Evidence Theory; Trust is calculated by observing the neighbour nodes' packet forwarding behavior.	Combining network security degree and correlation of time context, the trust computation is precise.	Need excess energy and time costs due to the cooperation and communication with neighbours. Memory costs also increase with network density. Energy costs to monitor the packet forward event of neighbour nodes.	On-Off attack.
	PLUS[35]	Weighting scheme, Trust is calculated based on personal reference and recommendation.	Efficiently detect malicious nodes.	Not suitable with high traffic rate, Trust convergence time is high, Computational complexity in implementing a set of recommendation protocols; Extra memory to store the recommendations.	Decrease the resource consumption that spend to reach destination

moved quickly. The probability theory needs significant memory and make the model process complex. the model is subject of spoofed, bad-mouthing attack and Syble attack, where the node compromised will propagates only good reputational information about the nodes [31], reputation system is the neighbor nodes' perception of its past behaviors. Based on related works [32, 33], the trust of the node is the neighbor nodes' belief about its future behaviors. In [34, 35], another distributed trust model was proposed, it's based in two techniques, the first is dealing with sensor availability and percentage of valid data packets. The second, computed based on number of sensors neighbor and their trust rating. The model success to detect fraudulent sensor in proper way. The model use hashing sequence number for all priority control information which caused more power consumption. The model is inefficient for WSNs high scale network. In [36], propose a model that has particular sensors for count positive and negative behavior of each sensor, the result was minimize the memory and computational complexity compared with same type of models. In WSNs environments, sometimes the sensor unit has several tasks to do with its neighbours, and need multi-trust rating corelated with the tasks, such this satiation. In[37], proposed a mechanism that maintain reputation for neighbor nodes for several different tasks and use the reputation to evaluate their trustworthiness. The model can be used in large scale WSNs. but the calculations based on Bayesian

TABLE II
DATA-BASED TRUST MODELS

	Scheme	characteristics	Prons	Cons	Features that addressed
Data-Based trust models	DFDI[41]	Distinguish Forged Data of Illegal nodes from innocent data of legal nodes, Weighting approach.	Mis-behaviour data from compromised nodes can be detected.	ECHO protocol consumes extra energy, time costs and suitable for only dense network.	Localization of neighbour nodes
	MDLC[43]	Weight approach, there are three states for sensor data raw, routed and processed.	Trust values calculated based on data life cycle. Minimal complexity.	Defense against trust model attacks.	The data trust based on the interactions between the neighbour's node.
	STM[46]	Trust value is based on consensus and consistency of data. Athematic mean is used to compare the value of data with other neighbour data.	New approach, simple and high level of accuracy in judgment.	Effectiveness and ability of the node not consider.	Minimum complexity, performance and scalability.
	TMCDE[45]	Beta Trust Model to determine the communication trust; Combine another model and the security data fusion algorithm to evaluate the trust of data.	Integration value based on communication trust, data trust and energy trust is more reliable.	Do not consider how to update trust values.	DoS attack

methods which mean that need more memory space and relatively caused computational complexity.

Data-Based trust models: The main job of sensor unit is sensing environments around the sensing unit, and their related process as well as management and control tasks. All those missions output is data, the models highlighted in previous section was ignored the data as source of trusting. However, most of threats are coming from the media between the sensors by attacking the wireless links, and we are aware the circumstances that can't be stronger enough against eavesdropping or any type of attacks that coming to the network through wireless link initially. The data trust models beginning in computer network are use the MAC to protect the integrity as in [38]. In [39], propose a different method by divide coverage area in grids with unique number each, and identify the node by verifying location [40, 41], and evaluate trustworthiness of their neighbor nodes by cross checking the neighbor nodes' redundant sensing data with their own result. It was used a weighted technique, the metric was measures are consistency, ability of the link and life time of the node. The model is suitable for the networks that has huge number of sensors, also its suffer from centralized mechanisms and assumes that the location of each sensor available which mean that reduced the network flexibility.

In [42], [43], a model based on data life cycle was proposed, they said there were three types of sensor data, raw, routed and processed. A value of each, was computed. The data trust based on the interactions between the neighbour's node is worthy if the data was in normal behaviour and if energy is equally expensed. In [44], [45], proposed model was consider the trust based on three factors, firstly the level of communication cooperation between node which can be computed by the number of successful transactions, secondly the level of the energy of the sensor and finally, the data consistency. It shoes effective resistance against DoS attack, once the energy level consumed in short time comparing to the normal power consumption. Sociopsychological trust model has been developed as in [46], it measure the trust as optimal value between ability of node and benevolence and integrity . consider of the ability of node as binary function if node is work or not, the benevolence was measure by comparing the node reading with the average neighbour's readings, and the integrity calculated by comparing the node reading with the

previous reading for the same node. when the trust value less than predetermine threshold, the immune module activates a process to isolate fraudulent node. Another version of Sociopsychological was proposed as in [47].

Miscellaneous Trust Models: In [48], proposed a model to secure data transmission, it's based on evaluate the node trust rate initially, then use the watermark techniques to detect the intruder that caused selective forwarding attack, the model set a number of trust for each sensor before node establish the network activity, that number is decrease in each time that the node behave fraudulent by half of that number. In [49] used watermark technique as conventional solution is not applicable in WSNs circumstances, since bulk message changes in continues form where by consume resources.

In [50] proposed similar technique with some advanced features such as dynamically detection the malicious behavior and direct the traffic towards trustworthy nodes. The drawback of this mechanism is that the sensor will continuously monitor its neighbour behavior, which impacted the sensor resources. In [51], propose a frame work, consider four models which are trust metric, behaviour detection, trust evaluation and trust aware routing. In [52] using utility theory concept to enhanced power consumption in such light-weight routing protocols, The comprehensive models work effectively against some attacks trade-off with energy cost and memory limitation. Aggregation in WSNs play a major factor to resume the loss in energy resources, reducing the high budget communication links can be achieved in such mechanism. Building the topology in hierarchal stricture is a type of such mechanism. This type of mechanism is subject of some attacks such as selective forwarding attack. In [53], present a model that provide three values of trusting, aggregation, forwarding, sensing. It come up with an idea for limit several attacks. In [54], an algorithm was present to mitigate the collision attack possibility, it show great accuracy and in performance as well. In [55], present a model using time series trust model and trust based auto regressive technique. The evaluation was, the proposed model defences of bad mouthing attack shows better performance.

B. Schemes Classified Based on Intelligent Methods

Recently, Computational Intelligence (CI) techniques are utilized widely to overcome of many issues in WSNs, Computational Intelligence is the study of adaptive mechanisms that enable or facilitate intelligent behaviour in complex and changing environments [56]. These mechanisms include paradigms that exhibit an ability to learn or adapt to new situations, to generalize, abstract, discover and associate. Paradigms categorized in five types and will highlight the most important researches related to trusting in WSNs.

Artificial Neural Networks: In [57], present how this science derivative from human neurology and types of models that resolved trusting problem in deferent aspects. It shows billions of neurons connected to each other to perform a precise task in very fast time. Also clarify the structure of artificial neural application in many WSNs aspects. In [58], proposed a model that used the formula of radial base (RBANN) as an activation function in neural network, to learn a model and expect future behaviour of a certain node, when the actual value is like what the system expect then the trust value will converge otherwise will diverge. The solution not shows any simulation or implementation that been consider. And the results only theoretical acceptable. In [59], present a model that used for intruder detection using the artificial neural network technique, the output of this study is study the model for several types of attacks and present a high true positive value.

Evolutionary Computation: In [60], proposed a model that used Evolutionary Game Theory (EGT) to detect the dynamic evolution of trust behavior. The output of research said that the diversity of trust sources is necessary to reach the efficient result. other game theoretic models of trust not been investigated. In [61], proposed a model that enhanced the velocity to reach stable state. In [62], replication dynamics in the model depicts the evolutionary that the model was assess and approved the theorems that was studied. In[63], an algorithm was developed in monitoring marine environment, comparison with similar algorithm, the model was more appropriate with respect to both optimization performance and computation time.

Swarm Intelligence: In [64], each sensor contains pheromone traces for its neighbours which determine probability for an ant to select a path. a set of artificial ants are created, and then they leave the clients sensors.

when an ant moves from sensor to another, it gives a command for these two sensors to modify the pheromone value of the path between them. if sensor has more neighbours not visited yet then compute average pheromone value of the path followed by ant from client to sensor. If its greater than threshold then ant stops and returns the solution. the output is either a sensor offering the requested service or not but having more neighbours not visited yet. the outcomes achieved good results but has weakness against insider threats. In [65], provide an effective security solution taking into account energy conservation. the Contribution is enhanced performance better than similar model. the Idea followed is enhanced version of [66] by add peer trust system. the research output is successfully increase accuracy with performance need to be enhanced. In [67], an efficient mechanisms that been tested to cluster head election process. Comparing with similar algorithms and show performance enhancing.

Artificial Immune System: In [68], Machine Learning Artificial Immune System (MLAIS) is proposed and use biological inspiration and machine learning techniques for adding security. the contribution of the research is to use intelligence trust mechanism to find the most reputable path leading to the most trustworthy node. The fraudulent nodes can be removed without affecting overall system. it mixture of machine learning module and immune model for detect up normal event and remove the node causal from the system. complexity in antigen and antibody concepts is highlighted trade-off with huge advantages in effectiveness of the model. In [69], present a mechanisms that called immune system-inspired routing recovery algorithm (ISRRA), aims to find the faulty routing and recovery that issue. It was utilizing several unit to achieve their goal, such as surveillance, response, learn and memory unit. The better performance highlighted as a kind contribution of the study. In [70], algorithm has been present performance measures average diagnosis latency, detection accuracy with respect to similar algorithms.

Fuzzy Systems: Linguistic variables include sometime uncertainty, need a system to decide exactly the meanings and weightings to interpret the human expert knowledge to machine language. Fuzzy mechanisms possess noteworthy interesting in intelligent trust researches in WSNs.

In [71], present a model that using fuzzy techniques can protect the IoT sensors against malicious behavior and selfish sensor. The model taking three inputs which are End-to-End packet forwarding ratio (EPFR), average energy consumption and packet delivery ratio (PDR). The detection probability is observed motivating results, with burden in memory storage.

In [72], Linguistic Fuzzy Trust Mechanism (LFTM) utilize bio-inspired (BTRM) trust model with using linguistic fuzzy reasoning. the contribution is maintaining the accuracy of the bio-inspired trust model, meanwhile enhancing the interpretability of the model. The model not tested in a wider spectrum of scenarios.

In [73], [74], a model that utilize Fuzzy Logic scheme is proposed to select best path to the packet destination. The system is taking the past behaviour of links about its intentions and norms. don't take in account the malicious node participation in the first study and covers in second. the performance is suffering from memory and power requirements.

Hybrid Paradigms: Since is no one of above paradigm superior to the others in all practical application in WSNs, hybrids of paradigms realize noteworthy results [56]. In [33], Node Behavior strategies Binding Belief Theory of Trust Evolution algorithm (NBBTE) proposed to integrate the approach of nodes behavioural strategies and modified evidence theory. the mechanism is Hybrid of FS and revised type of evidence combination rule. contribution of the study is combining network security degree and correlation of time context; the trust computation is precise. the result successfully understanding the fuzziness subjectivity and usability of trust. communication and cooperation with neighbours caused energy and time cost. memory costs are increases with network density. In [75], [76], AIS paradigm hybrid with SI was proposed. The inputs were treated are delay, energy level and another factor for maintain performance. The model not shows how to define against well-known attacks. The second study was relating to empirical study and achieve improvement in performance. In [77], ANN paradigm hybrid with Fuzzy logic system was present a model of cluster formation based on sensor characteristics. The model produced effective idea to reduce collision probability in high dense network. In [78], present intelligent real-time patient monitoring system for hospitals and provides a more accurate and reliable data for analysis.

C. Schemes Classified Based on Structral Methods

Based on information stored and process, the schemes categorized into Hierarchal, Distribution and Hybrid schemes. The advantages of hierarchal structure are least computational and memory usages, while disadvantages are communication overhead and issue with reliability and scalability. The distribution structure is most reliable and scalable, but the issue is with computational overhead. Hybrid structure has advantages that is less memory and less communication overhead, while has large computational overhead and large memory requirement than Hierarchal, less reliable and scalable compared to distributed.

It has been known that the clustering approaches is appropriate in WSNs environments from different aspects, saving bandwidth and increasing the lifetime of network is just a sample of their advantages in WSNs. In [79] Hybrid Trust Computation Scheme for Cluster-based WSNs (HTCW) was proposed and improve the model that has been developed by [80]. it is present the contribution to reduced cluster heads resources by specifically assign surveillance nodes to monitor nodes behaviours rather than CH nodes, the scheme is robust against some malicious attacks through rating cluster node behaviour and predict the future behaviour of the nodes. Although surveillance nodes can monitor the behaviours of cluster heads. They used data fusion and node revocation to measure the trustworthiness. CH in the model is very vulnerable to malicious attacks because the trust value of cluster heads is neglected. In [81]-[83], propose a hybrid trust computation scheme; named Group based Trust Management Scheme (GTMS), in which the whole group will get a single trust value. Within each group, all sensor nodes calculate individual trust values for all group members. the model provides protection against many malicious attacks, the model is minimal complexity, a different trying was proposed to improve the performance and the efficiency of the model.

V. Trust Best Practices

After the journey into literatures and corresponding analysis the following set of trust best practices recommend taking it in consideration:

1. Different trust computation for different task that node treatment.
2. Trust models should be simple as possible without enforcement in their capability, and detect different attacks by a clear idea, and prove it before establishing real operation.
3. Tiny devises were limitation in resources, but by thanks of huge advances in microelectronic industry and intelligence mechanisms, can perform high accurate function with high level of satisfaction.
4. Trust and reputation most calculated in same time since reputation is a node's opinion of other nodes in the network. Trust can be defined as the mathematical representation of reputation. Therefore, trust is a derivation of the reputation of an entity. Compare to calculating trust directly, using reputation to calculated trust can get a reliable trust value.
5. In order to improve the robustness of trust models, the related malicious attacked models which have been discussed in section 2 should be assessment.
6. Trust models should compute trust directly (first-hand information) way and indirect (second-hand information) independently. One of them only not enough for trust evaluation.
7. The balancing between WSNs task criticality level and risk can determine the best approach of trust that need to choose.

VI. Conclusions and Future Directions

In this paper, we presented a general survey of trust modeling in WSNs. Attacks and mitigations methods in WSNs were also reviewed. We firstly categorize all attacks related with trust schemes in WSNs from different aspects of attributes. an extensive literature survey is presented by summarizing the most advanced trust mechanisms in WSNs. In node-based trust mechanisms were ignored the node data as a source for trust computation, while most of attacks coming through the media between nodes, which can be detected when the node output monitored. The data-based trust mechanism is less reliable when the number of malicious node is increased, those type of models aims to provide integrity of node output. Another miscellaneous mechanism is based on the certain application provide it to network such as secure routing protocol, collect node location, secure data aggregation etc. we highlight most important of them.

Clustered based models are thanks of structure for saving power, least computational overhead, while has a lake of scalability. The flat models are more reliable and scalable but has a computational overhead and power consumption. The hybrid models are lese memory requirement than the cluster-based models but larger computational overhead than centralized models, and less reliable and scalable compared to flat models. Recently, intelligence model takes a high place in providing higher performance models, lower computational overhead, and lower energy consumption when works with hierarchal structure models. Many research investigated the appropriateness for each paradigm to specific challenge in WSNs, such as neural networks are most appropriate in design and deployment as well as evolutionary algorithms, and swarm intelligence, while fuzzy logic is most appropriate in security field and quality of service challenges, but moderately appropriate in routing clustering, scheduling, MAC and data aggregation. Based on the literature, the research gaps and the directions of future research are summarized. Current research is investigating in lightweight intelligence mechanisms. Future directions are in extending trust models into other type of WSNs platform, e.g. heterogeneous WSNs and dynamic WSNs.

References

[1] S. Döbelt, M. Busch, and C. Hochleitner, "Defining, Understanding, Explaining TRUST within the uTRUSTit Project," CURE, Vienna, Austria, Tech. Rep, 2012.

[2] F. Shahzad, M. Pasha and A. Ahmad, "A Survey of Active Attacks on Wireless Sensor Networks and their Countermeasures," Int. *J. Comput. Sci. Inf. Secur. (IJCSIS)*, vol. 14, no 12, pp. 54-65, Dec. 2016.

[3] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam and E. Cayirci, "Wireless sensor network: a survey," *Comput. Netw.*, vol. 38, no. 4, pp. 393-422, Mar. 2002, doi: 10.1016/S1389-1286(01)00302-4

[4] H. M. A. Fahmy, *Wireless sensor networks: concepts, applications, experimentation and analysis*, Singapore: Springer, 2016.

[5] V.P. Sai and V.R. Shyam, "Vampire Attacks: Draining Life From Wireless AD-Hoc Sensor Networks," *Int. J. Res. Comput. Commun. Technol. (IJRCCT)*, vol. 4, no. 8, pp. 586-593, 2015.

[6] A. Dubey, V. Jain and A. Kumar, "A Survey in Energy Drain Attacks and Their Countermeasures in Wireless Sensor Networks," *Int. J. Eng. Res. Technol. (IJERT)*, vol. 3, no. 2, Feb. 2014.

[7] W. Wang, Y. Lu and B. K. Bhargava, "On vulnerability and protection of ad hoc on-demand distance vector protocol," in *10th Int. Conf. Telecommun., 2003. ICT 2003.*, Papeete, Tahiti, French Polynesia, 2003, pp. 375-382 vol.1. doi: 10.1109/ICTEL.2003.1191259.

[8] R. Gill and M. Sachdeva, "Detection of Hello Flood Attack on LEACH in Wireless Sensor Networks," *in Next-Generation Networks*, D. K. Lobiyal, V. Mansotra and U. Singh, Eds, Singapore: Springer, 2018, pp. 377-387. doi: 10.1007/978-981-10-6005-2_40.

[9] A. Ramos, B. Aquino, R. H. Filho and J. J. P. C. Rodrigues, "Quantifying Node Security in Wireless Sensor Networks under Worm Attacks," Anais Principais Do Xxxv Simpósio Brasileiro De Redes De Computadores E Sistemas Distribuídos, SBC, May 2017.

[10] P. Sinha, V. K. Jha, A. K. Rai and B. Bhushan, "Security vulnerabilities, attacks and countermeasures in wireless sensor networks at various layers of OSI reference model: A survey," in *2017 Int. Conf. Signal Process. Commun. (ICSPC)*, Coimbatore, 2017, pp. 288-293. doi: 10.1109/CSPC.2017.8305855.

[11] B. Bhushan and G. Sahoo, "Recent Advances in Attacks, Technical Challenges, Vulnerabilities and Their Countermeasures in Wireless Sensor Networks," *Wirel. Pers. Commun.*, vol. 98, no. 2, pp. 2037-2077, Sept 8, 2017, doi: 10.1007/s11277-017-4962-0.

[12] Q. Wang, T. Nguyen, K. Pham and H. Kwon, "Mitigating Jamming Attack: A Game-Theoretic Perspective," in *IEEE Trans. Veh. Technol.*, vol. 67, no. 7, pp. 6063-6074, July 2018. doi: 10.1109/TVT.2018.2810865.

[13] P. Reindl, K. Nygard and X. Du, "Defending Malicious Collision Attacks in Wireless Sensor Networks," in *2010 IEEE/IFIP Int. Conf. Embed. Ubiquitous Comput.*, Hong Kong, 2010, pp. 771-776. doi: 10.1109/EUC.2010.121.

[14] M. Jo, L. Han, N. D. Tan and H. P. In, "A survey: energy exhausting attacks in MAC protocols in WBANs," *Telecommun. Syst.*, vol. 58, no. 2, pp. 153-164, Dec. 2014, doi: 10.1007/s11235-014-9897-0.

[15] S. Ramaswamy, H. Fu, M. Sreekantaradhya, J. Dixon and K. E. Nygard, "Prevention of Cooperative Black Hole Attack in Wireless Ad Hoc Networks," in *Int. Conf. Wirel. Netw.*, Las Vegas, NV, USA, 2003, pp. 570-575.

[16] Z. Zhang, S. Liu, Y. Bai and Y. Zheng, "M optimal routes hops strategy: detecting sinkhole attacks in wireless sensor networks," *Clust. Comput.*, vol. 22, no. 3, pp. 7677-7685, Mar. 2018, doi: 10.1007/s10586-018-2394-6.

[17] G. Jahandoust and F. Ghassemi, "An adaptive sinkhole aware algorithm in wireless sensor networks," *Ad Hoc Netw.*, vol. 59, pp. 24-34, May 2017, doi: 10.1016/j.adhoc.2017.01.002.

[18] D. R. Raymond and S. F. Midkiff, "Denial-of-Service in Wire-

less Sensor Networks: Attacks and Defenses," *IEEE Pervasive Comput*., vol. 7, no. 1, pp. 74-81, Jan.-March 2008. doi: 10.1109/MPRV.2008.6.

[19] P. Chawla and M. Sachdeva, "Detection of Selective Forwarding (Gray Hole) Attack on LEACH in Wireless Sensor Networks," in *Next-Generation Networks*, D. K. Lobiyal, V. Mansotra and U. Singh, Eds, Singapore: Springer, 2018, pp. 389-398. doi: 10.1007/978-981-10-6005-2_41.

[20] Y. Zhang and M. Minier, "Selective forwarding attacks against data and ack flows in network coding and countermeasures," *J. Comput. Netw. Commun*., vol. 2012, Nov. 2012, doi: 10.1155/2012/184783.

[21] R. Malik, H. Sehawat and Y. Singh, "Comprehensive Study of Selective Forwarding Attack in Wireless Sensor Networks," *Int. J. Adv. Res. Comput. Sci*., vol. 8, no, 9, pp. 1825-1838, May-June 2017, doi: 10.26483/ijarcs.v8i5.3876.

[22] W. D. Castell, A. D. Lewis, T. K. Ferguson, B. Yuan and I. M. Patterson, "Wireless Communication System Congestion Reduction Systemand Method," U.S. Patent 2007/0027956 A1, Fab. 1,2007.

[23] V. P. Illiano, L. Muñoz-González and E. C. Lupu, "Don't fool Me!: Detection, Characterisation and Diagnosis of Spoofed and Masked Events in Wireless Sensor Networks," *IEEE Trans. Dependable Secure Comput*., vol. 14, no. 3, pp. 279-293, 1 May-June 2017, doi: 10.1109/TDSC.2016.2614505.

[24] A. S. Naik and R. Murugan, "Security Attacks and Energy Efficiency in Wireless Sensor Networks: A Survey," *Int. J. Appl. Eng. Res*., vol. 13, no. 1, pp. 107-112, Nov. 2018.

[25] J. Newsome, E. Shi, D. Song and A. Perrig, "The Sybil attack in sensor networks: analysis & defenses," in *Third Int. Symp. Inf. Process. Sens. Netw*., 2004. IPSN 2004, Berkeley, CA, USA, 2004, pp. 259-268, doi: 10.1109/IPSN.2004.239019.

[26] D. Mohammed, M. Omar and V. Nguyen, "Wireless Sensor Network Security: Approaches to Detecting and Avoiding Wormhole Attacks," *J. Res. Bus. Econ. Manag. (JRBEM)*, vol. 10, no. 2, pp. 1860-1864, Feb. 2018.

[27] Y. -. Hu, A. Perrig and D. B. Johnson, "Packet leashes: a defense against wormhole attacks in wireless networks," in *IEEE INFOCOM 2003. (IEEE Cat. No.03CH37428)*, San Francisco, CA, 2003, pp. 1976-1986 vol.3, doi: 10.1109/INFCOM.2003.1209219.

[28] A. Diaz and P. Sanchez, "Simulation of Attacks for Security in Wireless Sensor Network," *Sens*., vol. 16, no. 11, Nov. 2016, doi: 10.3390/s16111932.

[29] W. Zhang, S. Zhu, J. Tang and N. Xiong, "A novel trust management scheme based on Dempster–Shafer evidence theory for malicious nodes detection in wireless sensor networks," *J. Supercomput*., vol. 74, no. 4, pp. 1779-1801, Sep. 2017, doi: 10.1007/s11227-017-2150-3.

[30] S. Ganeriwal, L. Balzano and M. B. Srivastava, "Reputation-based framework for high integrity sensor networks," *ACM Trans. Sens. Netw*., vol. 4, no. 3, pp. 1-37, June 2008, doi: 10.1145/1029102.1029115.

[31] Y. Yang, Q. Feng and Y. L. Sun, "RepTrap: a novel attack on feedback-based reputation systems," in *4th Int. Conf. Secur. Priv. Commun. Netw*., Istanbul, Turkey, Sept. 2008, doi: 10.1145/1460877.1460888.

[32] S. D. Wamvar, M. Schlosser and H. Garcia-Molina, "The Eigentrust algorithm for reputation management in P2P networks," in *12th Int. Conf. World Wide Web*, May 2003, pp. 640-651, doi: 10.1145/775152.775242.

[33] R. Feng, X. Xu, X. Zhou and J. Wan, "A Trust Evaluation Algorithm for Wireless Sensor Networks Based on Node Behaviors and D-S Evidence Theory," *Sens*., vol. 11, no. 2, pp. 1345-1360, doi: 10.3390/s110201345.

[34] Z. Yao, D. Kim and Y. Doh, "PLUS: Parameterized and Localized trUst management Scheme for sensor networks security," in *2006 IEEE Int. Conf. Mob. Ad Hoc Sens. Syst*., Vancouver, BC, 2006, pp. 437-446.

doi: 10.1109/MOBHOC.2006.278584.

[35] H. Safa, "A novel localization algorithm for large scale wireless sensor networks," *Comput. Commun*., vol. 45, pp. 32-46, June 2014, doi: 10.1016/j.comcom.2014.03.020.

[36] H. Chen, H. Wu, X. Zhou and C. Gao, "Agent-based Trust Model in Wireless Sensor Networks," in *Eighth ACIS Int. Conf. Softw. Eng. Artif. Intell. Netw. Parallel/Distributed Comput. (SNPD 2007)*, Qingdao, 2007, pp. 119-124. doi: 10.1109/SNPD.2007.122.

[37] H. Chen, "Task-based Trust Management for Wireless Sensor Networks," *Int. J. Secur. Appl*., vol. 3, no. 2, pp. 21-26, Apr. 2009.

[38] Fan Ye, Haiyun Luo, Songwu Lu and Lixia Zhang, "Statistical en-route filtering of injected false data in sensor networks," in *IEEE INFOCOM 2004*, Hong Kong, 2004, pp. 2446-2457 vol.4. doi: 10.1109/INFCOM.2004.1354666.

[39] J. Hur, Y. Lee, H. Yoon, D. Choi and S. Jin, "Trust evaluation model for wireless sensor networks," in *7th Int. Conf. Adv. Commun. Technol*., 2005, ICACT 2005., Phoenix Park, 2005, pp. 491-496, doi: 10.1109/ICACT.2005.245914.

[40] N. Sastry, U. Shankar and D. Wagner, "Secure verification of location claims," in *2nd ACM workshop Wirel. Secur*., Sept. 2003,

pp. 1-10, doi: 10.1145/941311.941313.

[41] G. Han, J. Jiang, L. Shu, J. Niu and H-C. Chao, "Management and applications of trust in Wireless Sensor Networks: A survey," *J. Comput. Syst. Sci.*, vol. 80, no. 3, pp. 602-617, May 2014, doi: 10.1016/j.jcss.2013.06.014.

[42] L. Gomez, A. Laube and A. Sorniotti, "Trustworthiness Assessment of Wireless Sensor Data for Business Applications,"in *2009 Int. Conf. Adv. Inf. Netw. Appl.*, Bradford, 2009, pp. 355-362, doi: 10.1109/AINA.2009.92.

[43] N. Haron, J. Jaafar, I. A. Aziz, M. H. Hassan and M. I. Shapiai, "Data trustworthiness in Internet of Things: A taxonomy and future directions," in *2017 IEEE Conf. Big Data Anal. (ICBDA)*, Kuching, 2017, pp. 25-30, doi: 10.1109/ICBDAA.2017.8284102.

[44] D. Hui-hui, G. Ya-jun, Y. Zhong-qiang and C. Hao, "A Wireless Sensor Networks Based on Multi-angle Trust of Node," in *2009 Int. Forum Inf. Technol. Appl.*, Chengdu, 2009, pp. 28-31, doi: 10.1109/IFITA.2009.71.

[45] F. Kazmi, M. A. Khan, A. Saeed, N. A. Saqib and M. Abbas, "Evaluation of trust management approaches in wireless sensor networks," in *2018 15th Int. Bhurban Conf. Appl. Sci. Technol. (IBCAST)*, Islamabad, 2018, pp. 870-875, doi: 10.1109/IBCAST.2018.8312329.

[46] H. Rathore, V. Badarla and G. K J, "Sociopsychological trust model for Wireless Sensor Networks," *J. Netw. Comput. Appl.*, vol. 62, pp. 75-87, Feb. 2016, doi: 10.1016/j.jnca.2015.09.009.

[47] H. Rathore, V. Bandarla and S. Shit, "Consensus-Aware Sociopsychological Trust Model for Wireless Sensor Networks," *ACM Trans. Sens. Netw.*, vol. 12, no. 3, July 2016, doi: 10.1145/2903721

[48] H. Deng, X. Sun, B. Wang and Y. Cao, "Selective forwarding attack detection using watermark in WSNs," in *2009 ISECS Int. Colloquium Comput. Commun. Control Manag.*, Sanya, 2009, pp. 109-113, doi: 10.1109/CCCM.2009.5268016.

[49] X. Yan, L. Zhang, Y. Wu, Y. Luo and X. Zhang, "Secure smart grid communications and information integration based on digital watermarking in wireless sensor networks," *Enterp. Inf. Syst.*, vol. 11, no. 2, pp. 223-249, Feb. 2017. doi: 10.1080/17517575.2015.1033767.

[50] P. R. Vamsi and K. Kant, "Self Adaptive Trust Model for Secure Geographic Routing in Wireless Sensor Networks," *Int. J. Intell. Syst. Technol. Appl.*, vol. 7, no. 3, pp. 21-28, Feb. 2015, doi: 10.5815/ijisa.2015.03.03.

[51] H. Deng, Y. Yang, G. Jin, R. Xu and W. Shi, "Building a Trust-Aware dynamic routing solution for Wireless Sensor Networks," in *2010 IEEE Globecom Workshops*, Miami, FL, 2010, pp. 153-157, doi: 10.1109/GLOCOMW.2010.5700197.

[52] P. Gong, T. M. Chen and Q. Xu, "ETARP: An Energy Efficient Trust-Aware Routing Protocol for Wireless Sensor Networks," *J. Sens.*, vol. 2015, Jan. 2015, doi: 10.1155/2015/469793

[53] N. Poolsappasit and S. Madria, "A Secure Data Aggregation Based Trust Management Approach for Dealing with Untrustworthy Motes in Sensor Network," in *2011 Int. Conf. Parallel Process.*, Taipei City, 2011, pp. 138-147, doi: 10.1109/ICPP.2011.16.

[54] M. Rezvani, A. Ignjatovic, E. Bertino and S. Jha, "Secure Data Aggregation Technique for Wireless Sensor Networks in the Presence of Collusion Attacks," in *IEEE Trans. Dependable Secure Comput.*, vol. 12, no. 1, pp. 98-110, 1 Jan.-Feb. 2015, doi: 10.1109/TDSC.2014.2316816.

[55] E. P. K. Gilbert, B. Kaliaperumal, E. B. Rajsingh and M. Lydia, "Trust based data prediction, aggregation and reconstruction using compressed sensing for clustered wireless sensor networks," *Comput. Electr. Eng.*, vol. 72, pp. 894-909, Nov. 2018, doi: 10.1016/j.compeleceng.2018.01.013.

[56] G. K. Kumar Venayagamoorthy, "A successful interdisciplinary course on coputational intelligence," in *IEEE Comput. Intell. Mag.*, vol. 4, no. 1, pp. 14-23, February 2009, doi: 10.1109/MCI.2008.930983.

[57] A. P. Engelbrecht, *Computational Intelligence*. 2nd ed, West Sussex, England: Wiley, 2007.

[58] A. Yasin and K. Sabaneh, "Enhancing Wireless Sensor Network Security using Artificial Neural Network based Trust Model," *Int. J. Adv. Comput. Sci. Appl.*, vol. 7, no. 9, pp. 222-228, 2016. doi: 10.14569/IJACSA.2016.070932.

[59] C. D. Mcdermott and A. Petrovski, "INVESTIGATION OF Computational Intelligence Techniques For Intrusion Detection In Wireless Sensor Networks," *Int. J. Comput. Netw. Commun.*, vol. 9, no. 4, Jul. 2017, doi: 10.5121/ijcnc.2017.9404.

[60] C. A. Kamhoua, N. Pissinou and K. Makki, "Game Theoretic Modeling and Evolution of Trust in Autonomous Multi-Hop Networks: Application to Network Security and Privacy," in *2011 IEEE Int. Conf. Commun. (ICC)*, Kyoto, 2011, pp. 1-6, doi: 10.1109/icc.2011.5962511.

[61] Y. Li, H. Xu, Q. Cao, Z. Li and S. Shen, "Evolutionary Game-Based Trust Strategy Adjustment among Nodes in Wireless Sensor Networks," *Int. J. Distrib. Sens. Netw.*, vol. 11, no. 2, Feb. 2015, doi: 10.1155/2015/818903.

[62] S. Shen, L. Huang, E. Fan, K. Hu, J. Liu and Q. Cao, "Trust Dynamics in WSNs: An Evolutionary Game-Theoretic Approach," *J. Sens.*, vol. 2016, Apr. 2016, doi: 10.1155/2016/4254701.

[63] B. Cao, J. Zhao, P. Yang, Z. Lv, X. Liu and G. Min, "3-D Multiobjective Deployment of an Industrial Wireless Sensor Network

for Maritime Applications Utilizing a Distributed Parallel Algorithm," in *IEEE Trans. Ind. Inform.*, vol. 14, no. 12, pp. 5487-5495, Dec. 2018, doi: 10.1109/TII.2018.2803758.

[64] M. Dorigo, M. Birattari and T. Stutzle, "Ant colony optimization," in *IEEE Comput. Intell. Mag.*, vol. 1, no. 4, pp. 28-39, Nov. 2006, doi: 10.1109/MCI.2006.329691.

[65] H. Marzi and M. Li, "An Enhanced Bio-inspired Trust and Reputation Model for Wireless Sensor Network," *Procedia Comput. Sci.*, vol. 19, pp. 1159-116, June 2013, doi: 10.1016/j.procs.2013.06.165.

[66] Li Xiong and Ling Liu, "PeerTrust: supporting reputation-based trust for peer-to-peer electronic communities," in *IEEE Trans. Knowl. Data Eng.*, vol. 16, no. 7, pp. 843-857, July 2004, doi: 10.1109/TKDE.2004.1318566.

[67] P. C. S. Rao, P. K. Jana and H. Banka, "A particle swarm optimization based energy efficient cluster head selection algorithm for wireless sensor networks," *Wirel. Netw.*, vol. 23, no. 7, pp. 2005-2020, Oct. 2017, doi: 10.1007/s11276-016-1270-7.

[68] H. Rathore, V. Badarla, S. Jha and A. Gupta, "Novel approach for security in Wireless Sensor Network using bio-inspirations," *2014 Sixth Int. Conf. Commun. Syst. Netw. (COMSNETS)*, Bangalore, 2014, pp. 1-8, doi: 10.1109/COMSNETS.2014.6734875.

[69] X. Zhang , G. Yao, Y. Ding and K. Hao, "An improved immune system-inspired routing recovery scheme for energy harvesting wireless sensor networks," *Soft Comput.*, vol. 21, no. 20, pp. 5893-5904, Oct. 2017, doi: 10.1007/s00500-016-2222-y.

[70] S. Mohapatra and P. M. Khilar, "Artificial immune system based fault diagnosis in large wireless sensor network topology," in *TENCON 2017 - 2017 IEEE Region 10 Conf.*, Penang, 2017, pp. 2687-2692, doi: 10.1109/TENCON.2017.8228317.

[71] C. Dong, C. Guiran, S. Dawei, L. Jiajia, J. Jie and W. Xingwei, "TRM-IoT: A trust management model based on fuzzy reputation for internet of things," *Comput. Sci. Inf. Syst.*, vol. 4, no. 4, pp. 1207-1228, 2011, doi: 10.2298/CSIS110303056C.

[72] F. G. Mármol, J. G. Marín-Blázquez and G. M. Pérez, "LFTM, linguistic fuzzy trust mechanism for distributed networks," *Concurr. Comput. Pract. Exp.*, vol. 24, no. 17, Aug. 2011, doi: 10.1002/cpe.1825.

[73] T. K. Kim and H. S. Seo, "A Trust Model using Fuzzy Logic in Wireless Sensor Network," *World Acad. Sci., Eng. Technol.*, vol. 42, no. 6, pp. 63-66, Aug. 2008.

[74] R. A. Raje and A. V. Sakhare, "Routing in Wireless Sensor Network Using Fuzzy Based Trust Model," in *2014 Fourth Int. Conf. Commun. Syst. Netw. Technol.*, Bhopal, 2014, pp. 529-532, doi: 10.1109/CSNT.2014.111.

[75] K. Saleem, N. Fisal, S. Hafizah, S. Kamilah and R. Rashid, "Biological inspired self-optimized routing algorithm for wireless sensor networks," in *2009 IEEE 9th Malaysia Int. Conf. Commun. (MICC)*, Kuala Lumpur, 2009, pp. 305-309, doi: 10.1109/MICC.2009.5431519.

[76] K. Saleem, N. Fisal and J. Al-Muhtadi, "Empirical Studies of Bio-Inspired Self-Organized Secure Autonomous Routing Protocol," *IEEE Sens. J.*, vol. 14, no. 7, pp. 2232-2239, July 2014, doi: 10.1109/JSEN.2014.2308725.

[77] K. N. Veena and B. P. V. Kumar, "Dynamic clustering for Wireless Sensor Networks: A Neuro-Fuzzy technique approach," in *2010 IEEE Int. Conf. Comput. Intell. Comput. Res.*, Coimbatore, 2010, pp. 1-6, doi: 10.1109/ICCIC.2010.5705748.

[78] K. Singh, D. Sharma and S. Aggarwal, "A Real Time Patient Monitoring System based on Artificial Neural Fuzzy Inference System (ANFIS)," *Int. J. Comput. Appl.*, vol. 146, no. 15, pp. 22-28, Jul. 2016, doi: 10.5120/ijca2016910959.

[79] P. Neamatollahi, S. Abrishami, M. Naghibzadeh, M. H. Yaghmaee Moghaddam and O. Younis, "Hierarchical Clustering-Task Scheduling Policy in Cluster-Based Wireless Sensor Networks," *IEEE Trans. Ind. Inform.*, vol. 14, no. 5, pp. 1876-1886, May 2018, doi: 10.1109/TII.2017.2757606.

[80] Y. Zhou, T. Huang and W. Wang, "A Trust Establishment Scheme for Cluster-Based Sensor Networks," in *2009 5th Int. Conf. Wirel. Commun., Netw. Mob. Comput.*, Beijing, 2009, pp. 1-4, doi: 10.1109/WICOM.2009.5302528.

[81] R. A. Shaikh, H. Jameel, Sungyoung Lee, S. Rajput and Young Jae Song, "Trust Management Problem in Distributed Wireless Sensor Networks," in *12th IEEE Int. Conf. Embed. Real-Time Comput. Syst. Appl. (RTCSA'06)*, Sydney, Qld., 2006, pp. 411-414, doi: 10.1109/RTCSA.2006.61.

[82] R. A. Shaikh, H. Jameel, B. J. d'Auriol, H. Lee, S. Lee and Y. Song, "Group-Based Trust Management Scheme for Clustered Wireless Sensor Networks," in *IEEE Trans. Parallel Distrib. Syst.*, vol. 20, no. 11, pp. 1698-1712, Nov. 2009, doi: 10.1109/TPDS.2008.258.

[83] S. Che, R. Feng, X. Liang and X. Wang, "A lightweight trust management based on Bayesian and Entropy for wireless sensor networks," *Secur. Commun. Netw.*, vol. 8, no. 2, Mar. 2014, doi: 10.1002/sec.969.