International Journal of Electrical and Computer Engineering (IJECE)
Vol. 11, No. 2, April 2021, pp. 1375∼1387
ISSN: 2088-8708, DOI: 10.11591/ijece.v11i2.pp1375-1387

A trust-based authentication framework for security of WPAN using network slicing

Sazia Parvin[1], Amjad Gawanmeh[2], Sitalakshmi Venkatraman[3], Ali Alwadi[4], Jamal N. Al-Karaki[5], Paul D. Yoo[6]

[1,3]Melbourne Polytechnic, Victoria, Australia
[2]Department of Electrical Engineering, College of Engineering and IT, University of Dubai, Dubai, United Arab Emirates
[4]School of Engineering, Auckland University of Technology Auckland, New Zealand
[5]Department of Information Security Engineering Technology, Abu Dhabi Polytechnic, Abu Dhabi, United Arab Emirates
[5]Department of Computer Engineering, The Hashemite University, Zarqa-Jordan
[6]Department of Computer Science and Information Systems, Birkbeck College, University of London, London, United Kingdom

Article Info

Article history:

Received Apr 25, 2020
Revised Aug 7, 2020
Accepted Aug 18, 2020

Keywords:

Authentication
Security
Substantiality
Trust
WPAN

ABSTRACT

New technologies and their seamless wireless interconnectivity bring along many challenges including security and privacy issues that require immediate attention. Wireless personal area networks (WPANs) are characterized by limited energy resources and computing power which call for lightweight security mechanisms in these networks as a mandatory requirement. In this paper, a lightweight trust-based framework for node authentication in WPAN is proposed. Our main objective is to minimise the effort in distinguishing valid requests of trustworthy nodes from invalid requests of malicious nodes that can result in network compromises. We achieve this through network slicing which divides the network into primary and secondary virtual networks. The proposed framework has three-fold benefits. Firstly, it authenticates nodes' requests based on a novel method of trust value calculation. Secondly, the framework maintains energy efficiency while authenticating nodes' requests to access WPAN resources. Finally, the framework provides a solution for the biasing problem that can arise due to unexpected behaviour of malicious users in WPANs. The framework efficacy is illustrated by using a case study to show how it can accurately capture trust relations among nodes while preventing malicious behavior.

Corresponding Author:

Amjad Gawanmeh
College of Engineering and IT
University of Dubai, Dubai, UAE
Email: amjad.gawanmeh@ud.ac.ae

1. INTRODUCTION

Recent rapid advancements in wireless communications, sensor technologies, and the Internet of things (IoT) have resulted in the evolution of wireless body area network (WBAN) and wireless personal area networks (WPAN) into an interdisciplinary networking paradigm, connecting people with various real-time applications including healthcare, sports, entertainment and social media [1–5]. WPAN is a very common and prevailing technology that is used to monitor and collect data from a physical environment through sensors that can be attached to the person, implanted, or deployed around the person's confined area. While a WBAN interconnects independent nodes (e.g. sensors and actuators) that are present in, on, or around a human body, a

WPAN is a connected network of devices centered on an individual's personal workspace. Due to their inherent limitations in memory and power, they are vulnerable to malicious attacks since current security solutions are not suitable to protect each node as well as dynamic topology of distributed data processing in WSN [6, 7].

Weak security in WSN can have an adverse impact that could even result in life-threatening conditions in healthcare [6]. In addition, different types of short range wireless networks are constantly expanding with various devices attached as demonstrated in [8]. The various types of WPANs applications raises several issues related to preserving data confidentiality and privacy [9]. With the increased use of WPANs in various applications that can impact both personal and professional life, it is important to build a lightweight trust-based authentication framework for ensuring their security [10, 11]. With this aim, the focus of this research is to propose a security framework to safeguard WPAN with a simplified and lightweight trust management mechanism. Several studies have demonstrated the feasibility of security attacks on these types of networks [12], thus, WPAN is considered as a threat by individuals due to the existing vulnerabilities in protecting their personal data and privacy [13].

Traditional authentication and trust management methods of WPAN are ineffective and the current security situation warrants an efficient lightweight security method with minimum overhead. Such a solution must address several security concerns in WPANs: i) a malicious node in WPAN could abuse its resources with selfish behavior; ii) a malicious node treated as a primary user could stop secondary nodes from using the network; and iii) malicious nodes could create biased nodes with traditional trust management schemes as their true trust values are not known. While trust in WPAN has been discussed in the current state of the art [14], the method applied are not suitable for WPAN. Firstly, most trust-based schemes are applied only for routing problem in WPANs and not for prevention of access to untrustworthy node. Secondly, due to the difficulty in calculating the true trust values for biased nodes for authentication in WPAN context, there is paucity of research to address this problem. Finally, to the best of our knowledge, no solution for authentication in WPAN using trust management scheme exists to enhance security in WPANs using network slicing, where nodes belong to either a primary or a secondary virtual group.

Several methods were proposed to address security in wireless application oriented networks, including the work reported in [8], which addressed the issue of detecting impersonation attack in wireless WiFi. Recently, time-bound lightweight frameworks that are services-based in processing security policies are studied [15]. Some security approaches are tool-based and focus on the network routing protocols as well as authentication and encryption techniques [16]. Existing WPAN security methods are predominantly limited in solving a specific problem [17, 13]. Many new models and metrics for trust evaluation proposed are not generic and consider specific location-based privacy, backward broadcasting or tunnelling issues [18, 19]. Such schemes require hybrid security architectures that use different algorithms for different problems. In previous work, Sazia *et al.* [20] proposed trust-based authentication mechanism in cognitive radio networks (CRNs) to secure the spectrum sharing process. However, it did not address trust-biasing problem. Subsequently, Sazia *et al.* [21] proposed a community-based grouping technique to ensure the trust-based authentication process in CRNs, and in [22] secondary node authentication in WBAN was introduced. However, it lacked the proof of trust evaluation for authentication. Trust is important as it is a measure of a node's reliability and security within the network throughout its communication with other nodes. Other works have limited focus of trust in healthcare applications for quality of data delivery and network operations [23].

This paper aims to address the issue of node authentication in WPANs in general. It proposes a novel lightweight method that can enhance the security of WPAN taking into consideration the topology and nature of the network paradigm. Existing solutions are resource extensive while WPAN do not have computational power. Further, some nodes or implanted devices are difficult to be maintained with limited power supply, and WPANs have dynamic and mobile characteristics. So far, WPAN can only support low security requirement applications, such as athletes' wearables, and critical applications, such as continuous heart monitoring devices. These form our research motivation in proposing a reliable lightweight security mechanism for node authentication in WPANs.

2. NODE AUTHENTICATION IN WPANS BASED ON TRUST

In WPAN/WBAN, the sensors and devices might be wearable, implanted or used for personal monitoring. Such sensors and monitoring devices are usually designed with minimal complexity and low power consumption in order to maximize battery life. However, existing security primitive operations, such as hash-

ing and encryption, require powerful processing and high resources making them unsuitable for these sensors and devices. Therefore, in this paper, we propose a lightweight framework for trust management and authentication of nodes in WPAN. The framework treats the WPAN as cognitive radio enabled wireless network, and divides nodes into two types, primary user (PU) and secondary user (SU). PU is a trusted node in WPAN that is physically secure, and SU is a node that cognitively operates through the WPAN without causing harmful interference to the PU. In addition, there is a device that allows other wireless devices to connect to a wired or wireless network using WiFi, or related standards. In addition, Further, our framework consists two units called base stations, the primary user base station (PUBS) and secondary user base station (SUBS).

2.1. System model and architecture

Figure 1 depicts the proposed trust based authentication WPAN architecture by dynamically dividing nodes into two groups: primary and secondary. This architecture fits well for WPAN due to the mobility of the network and the dynamics of its topology that allows nodes to be part of the network based on several aspects, including time, and location.

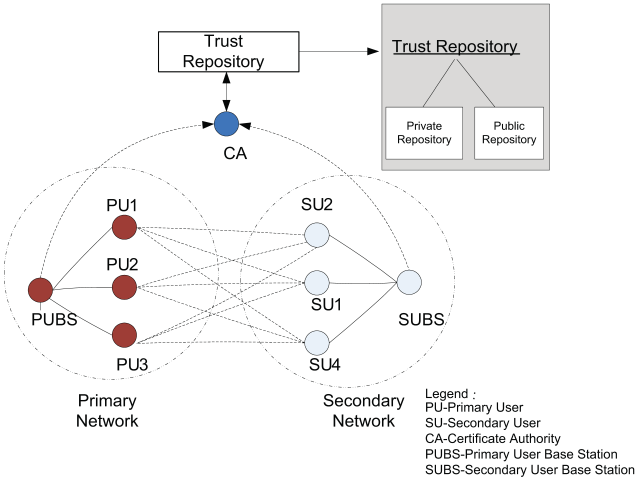

Figure 1. System architecture for the trust-based authentication framework for WPAN/WBAN

The key components of the framework include the (Base station) which acts as a point of contact between primary nodes as well as secondary nodes. The architecture contains on primary user base station (PUBS) that connects primary nodes, and a secondary user base station (SUBS) that connects secondary nodes. In addition, the certificate authority (CA) is used to maintain trust values for all nodes as well as for updating the trust repository whenever requested from the PUBS or SUBS. In addition, it plays a role in the authentication process. Finally, Trust repository acts as a database for nodes' trust values. Since the trust value is publicly known, its integrity is achieved storing a private trust value for every node locally. The private trust value is only visible to the CA so that it can be validated against any malicious modification.

2.2. Operation of trust-based authentication framework

This section shows how nodes can join the WPAN as secondary nodes using the proposed architecture. Figure 2 shows the steps, where the node request is made by the node to the WPAN. The request is processed into the BS, which in turn calculates a trust value for the node, and communicate it with the CA. The CA first checks for biasing, and if detected, the biasing algorithm is used to handle this situation. Otherwise, the authentication decision is made based on the calculated trust value. The decision is communicated, and the trust value is updated if necessary.

The first step of the proposed method is to perform trust calculation for candidate nodes. When a node wants to use the network resources i.e. as a secondary node, the SUBS calculates its corresponding trust value. this is achieved by asking all member nodes of the SUBS to assign a trust value to the candidate node. Once every member communicates back its recommended value, based on history of the node, the SUBS aggregates the received trust values and obtains one for the candidate node. If the node is deemed trustworthy, then it is either authenticated by the SUBS or the request is forwarded to the PUBS. In this case, the PUBS

also calculates the candidate node's trust value to decide its eligibility to access the required resources. This is done through the trust based authentication framework process as shown in Figure 2. Any calculated trust value of the candidate node must be communicated to the CA to process it. Once a trust value is calculated, authentication process is started. Authentication is performed based on trust value and a predefined threshold. While processing trust value through the CA, a biasing check is performed, if the calculated trust value is found biased, then SUBS handle this situation by marking nodes with improper trust value is biased. Trust calculation, authentication, and biasing are discussed in more detail in the following two sections.

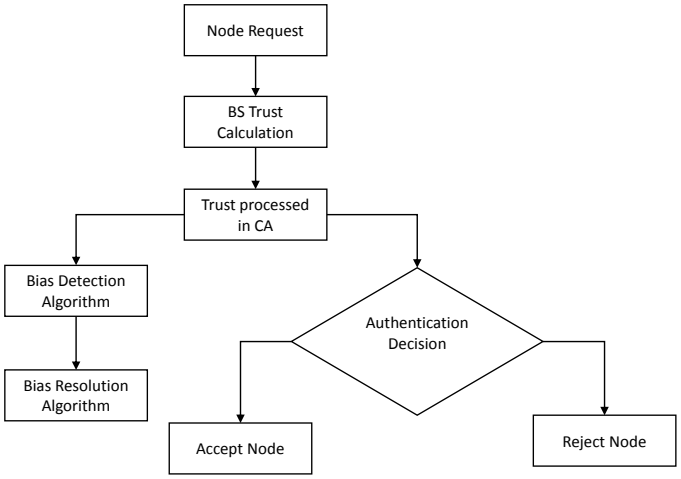

Figure 2. Trust based authentication framework

3. TRUST EVALUATION

In a real life scenario, large number of connected devices, such as wearable devices, smart devices, WBSN nodes, devices with tags, etc get connected dynamically making trust calculation becomes a continuous process. We define trust in WPAN as a degree of reliability and security that can be ensured when a SU requests to access any PU's node. In this context, trust is calculated for authenticating a SU's request and to determine whether the SU can be allowed to use a PU's free spectrum or other network resources without causing any security breach or malicious attack in the WPAN. In our proposed framework, we calculate the candidate SU node's trust comprehensively using the direct trust, indirect trust and integrated trust evaluation models, which are described next. Our proposal differs from the methods adopted in literature [24, 25] as it is uniquely modeled for WPAN. Figure 3 shows a scenario for trust evaluation models in our proposed framework by depicting the different trust relationships between a candidate SU node and other member PU nodes. The trust values calculated using three trust evaluation models, namely direct trust, indirect trust and integrated trust, with trust values are in the range of 0 (complete distrust) and 1 (complete trust). In the next subsections, we explain the process adopted in calculating the candidate node's trust value using various scenarios of the member node relationships established.

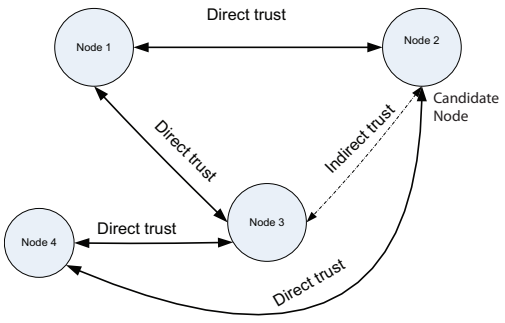

Figure 3. A scenario for trust evaluation models

3.1. Direct trust value calculation

In this model, we evaluate the direct trust of a candidate node by proposing a computation method for determining a quantitative direct trust value. The direct trust value of a node is calculated by other member nodes if a direct relationship has been established between them via some past interaction and cooperation experiences. Let us denote the direct trust value as $T_{Directtrust}$. In Figure 3, node 2 represents the candidate SU node, and it has established direct communication links with both node 1 and node 4. Hence, node 1 and node 4 will use the direct trust evaluation model based on the past communication link to calculate the candidate node's trust value.

A candidate node's direct trust value is determined based on the member nodes that have established a direct communication link or cooperation. In a dynamic WPAN, the relationships between nodes keep changing. Hence, the trust values determined by the member nodes have to be constantly monitored by the base station according to the users' multi-attribute trust values. A historic record of information about all the past communication links established are maintained in a table of cooperation records as shown in Table 1. The candidate node's trust value is calculated based on its attribute values. In our proposed approach, each attribute has three values associated, namely the number of successes $(S_i, i = 1, 2....n)$, the number of failures $(F_i, i = 1, 2...n)$ and the amount of cooperation $(C_i, i = 1, 2, ...n)$. We assume equal values assigned between the users for cooperative/non-cooperative behavior during their interaction process.

Table 1. Cooperation record table

Attributes	Success	Failure	Cooperation Sum
A_1	S_1	F_1	C_1
A_2	S_2	F_2	C_2
....	....	....	....
A_n	S_n	F_n	C_n

We define the cooperation sum used in Table 1 as the total sum of the number of successes and failures of a candidate node's request or event and is represented by $C_i = S_i + F_i, i = 1, 2, ...n$. The trust value for attribute A_i can be computed based on the values in Table 1 and then can be used to calculate the candidate node's overall trust value (denoted by $T_{Directtrust}$) with n attributes $A_i, i = 1, 2, ..n$ by combining the trust values for each attribute T_{A_i} as follows:

$$T_{Directtrust} = \frac{\sum_{i=1}^{n} T_{A_i}}{\sum_{i=1}^{n} T_{A_i} + \sum_{i=1}^{n} (1 - T_{A_i})}, \; where \; T_{A_i} = \frac{S_i}{C_i}, \tag{1}$$

3.2. Indirect trust value calculation

In order to evaluate the indirect trust of a candidate node in the absence of any direct communication link with another node, we consider the recommendations from the neighboring member nodes. The past interactions between the surrounding member nodes and the candidate node is used to establish the indirect trust value of the candidate node. In this model, each member node that does not have any past communication link or cooperation experience with the candidate node will then make a request to other neighboring member nodes for providing recommendations about the candidate node. By this method, the candidate node's trust is calculated indirectly Let us denote such an indirect trust value as $T_{Indirecttrust}$. As shown in Figure 3, node 3 has no direct communication link with the candidate node (node 2). However, node 3 has a direct communication with node 1 and node 4. Hence, node 3 can facilitate a request to node 1 and node 4 to make a recommendation about the candidate node. Therefore, the indirect trust evaluation model will be adopted for node 3 to compute the candidate node's trust value.

According to the second scenario of our trust evaluation model, where the member node does not have direct communication link or cooperation established with the candidate node, an indirect trust value is calculated. In this case, the member node makes a request to other neighboring member nodes for recommendations about the candidate node. We divide these surrounding nodes into three different types, namely reliable nodes (trustworthy nodes), unknown nodes and unreliable nodes. Reliable nodes are those surrounding nodes that have provided trustworthy recommendations in the past. Let $(T_{reliable})$ denote the trust value recommended

by such reliable nodes. Unknown nodes are those surrounding nodes from whom the member node has not solicited recommendations in the past. Let $(T_{unknown})$ represent the trust value recommended by these unknown nodes. Based on history of events, if a neighboring node has provided incorrect recommendations in the past, it is considered as an unreliable node. Let $(T_{unreliable})$ denote the trust value recommended by unreliable nodes. In the Indirect Trust value calculation, the member node considers the recommendations from reliable and unreliable nodes only and not from the unreliable nodes. In addition, a weight factor which represents the degree of utility/importance based on the events that were monitored and quantified are given to distinguish between the recommendations from reliable and unknown nodes. It is logical to expect a higher weight factor assigned to reliable nodes' recommendations as that of unknown nodes. The trust values of both $T_{reliable}$ and $T_{unknown}$ are required to be first calculated in order to determine the candidate node's Indirect Trust value.

The process of calculating trust value from reliable nodes consists of two steps: i) the member node retrieves the trust values stored locally from the reliable nodes they have directly evaluated; and ii) the member node receives trust values from reliable nodes who have provided the recommendations about the candidate node's trust value. The member node combines all these trust values and computes $T_{reliable}$ using 2.

$$T_{reliable} = \frac{\sum_{i=1}^{n_{reliable}} T_{MR_i} \times T_{RC_i}}{n_{reliable}} \tag{2}$$

where T_{MR_i} denotes the trust value from member node (M) to i th reliable node (R);
T_{RC_i} denotes the trust value from reliable node (R) to candidate node (C) and
$n_{reliable}$ denotes the total number of reliable nodes.

Next, the trust values from unknown nodes $T_{unknown}$ are calculated using 3.

$$T_{unknown} = \frac{\sum_{k=1}^{n_{unknown}} T_{UC_k}}{n_{unknown}} \tag{3}$$

where T_{UC_k} denotes the trust value from kth unknown node to candidate node and
$n_{unknown}$ denotes the total number of unknown nodes.

Let us denote a weight $W_{reliable}$ to be allocated to the reliable nodes' trust value $T_{reliable}$ and a weight $W_{unknown}$ to be assigned to unknown nodes' trust value $T_{unknown}$. We use the approach given in [Reference thesis] to allocate the weights, $W_{reliable}$ and $W_{unknown}$.

We adopt the traditional weighted approach to calculate the candidate node's overall Indirect Trust value as follows, where $W_{reliable} + W_{unknown} = 1$ and $W_{reliable}, W_{unknown} \in [0, 1]$:

$$T_{Indirecttrust} = T_{reliable}W_{reliable} + T_{unknown}W_{unknown} \tag{4}$$

3.3. Integrated trust value calculation

It is typical that WPAN exhibits dynamic situations from time to time, establishing direct as well as indirect communication links between the nodes. An integrated trust evaluation model is proposed here for situations where both direct and the indirect trust values have been computed. In this model, we combine both direct trust and indirect trust values from member nodes in order to compute the candidate node's overall trust value indirectly. Let us denote the integrated trust value as T_{ig}. In Figure 3, both node 1 and node 4 has established both direct and indirect communication links with the candidate node (node 2). Therefore, node 1 and node 4 will adopt the integrated trust evaluation model to combine the direct trust as well as Indirect Trust values computed from both links for determining the candidate node's overall trust value.

In the third scenario of trust evaluation model of our proposed framework, the Integrated Trust value of a candidate node is calculated for situations when the candidate node has established both direct and indirect communication links with member nodes. In this case based on the requirements of a certain task, each member node assigns different weights using the weighted approach. Let us denote W_{dt} as the weight for the direct trust value and W_{it} as the weight for the indirect trust value. Then, the candidate node's Integrated Trust value is calculated by the following equation, where $W_{dt} + W_{it} = 1$ and $W_{dt}, W_{it} \in [0, 1]$

$$T_{ig} = W_{dt} \times T_{dt} + W_{it} \times T_{it} \tag{5}$$

These calculations determine if a cooperation between nodes have taken place and each member node updates the Integrated Trust value of its cooperation node (candidate node) accordingly. The SUBS can now make a decision on an SU's request to authenticate access to PU's network based on the above calculated trust value. While the above trust evaluation model works for existing SU in the network, it does not cater to situations when a new user who has securely joined a secondary network of the WPAN makes a request to access the PU's network, This is because the trust value may not be available with the PUBS or other PUs. Hence, we propose a bootstrapping method to address such a new SU case scenario in the next subsection.

3.4. Bootstrapping of trust value calculation

We propose a bootstrapping method for the PUBS to determine the trust value for a newly joined SU under two main methods: i) Triangular Trust value calculation; and ii) Reference Trust value calculation. The algorithm for bootstrapping a new SU's trust value is provided in the following three steps:

- A newly joined SU requests the SUBS to access the PU's free spectrum. This request is subjective to the trust value determined by the SUBS and is based on: i) its joining process to the secondary network; and ii) its behaviour pattern observed for a certain period of time. On successful completion of this authentication process, the SUBS sends the request to the PUBS for further action.
- When the PUBS receives the request from the SUBS for the SU to access the primary network, the authentication is based on the SU's trust value. At this stage, since the SU node has no trust value with either the PUBS or the other PUs, triangular trust value calculation method is invoked, which is based on the trust relationship between the PUBS and SUBS.
- There are two pathways: i) a trust relationship exists between PUBS and SUBS-SU's trust value is based on the triangular trust value calculation method; or ii) no trust relationship exists between the SUBS and PUBS-trustworthy member nodes in the secondary network are used by the PUBS and the SU's trust value is based on reference trust value calculation method.

We provide a detailed algorithm of trust value calculations under both triangular trust and reference trust methods in the following subsections.

3.4.1. Triangular trust value calculation

This bootstrapping method is used when some trust relationship exists between the SUBS and PUBS. The triangular trust calculation method is used here to determine the trust value of a new SU when it has a relationship with the SUBS but not with the PUBS. Let us assume the trust relationship between PUBS $\longrightarrow$ SUBS; SUBS $\longrightarrow$ SU1 for calculating the trust value of the SU node (SU1), and denote $T_{PUBS,SU1}$ as the trust value of the PUBS for the SU node (SU1). Assuming the trust value between PUBS and SUBS to be 0.8, and the trust value between SUBS and SU1 to be 0.7, we have $T_{PUBS,SUBS} = 0.8$ and $T_{SUBS,SU1} = 0.7$, we can calculate the Triangular Trust value between the PUBS and SU1 as follows:

$$T_{PUBS,SU1} = T_{PUBS,SUBS} * T_{SUBS,SU1} = 0.8 * 0.7 = 0.56$$

3.4.2. Reference trust value calculation

This bootstrapping method is used in cases where there is no relationship between PUBS and SUBS. The reference trust value calculation for a newly joined SU is based on the recommendations from other users. The difference here from the indirect trust value calculation method is that the SUs and not the PUs request for recommendations from the PUBS. Here, various trust values received are collected and the average of these values are computed to determine the overall trust value for the new SU. As shown in Figure 4, let us assume the trust relationship between different nodes such that PUBS trusts SU2 and SU3 with a value of 0.5 and 0.6, respectively, and SU1 who is a newly joined SU has a trust value of 0.5 with SU2 and 0.4 with SU3. In this case, the average trust value between the PUBS and SU1 is determined as follows:

$$T_{PUBS,SU1} = (T_{PUBS,SU2} * T_{SU2,SU1} + T_{PUBS,SU3} * T_{SU3,SU1}))/2 = (0.5 * 0.5 + 0.6 * 0.4)/2 = 0.249 \Longrightarrow 0.25$$

Finally, the PUBS decides to declare whether the SU node (SU1) is trustworthy or not based on whether the above computed trust value (either through Triangular Trust relationship or Reference Trust relationship) is greater than the predefined threshold value $(T_{threshold})$ or not. Hence, the predefined threshold value plays a major role in determining the minimum level of trust required by the PUBS.

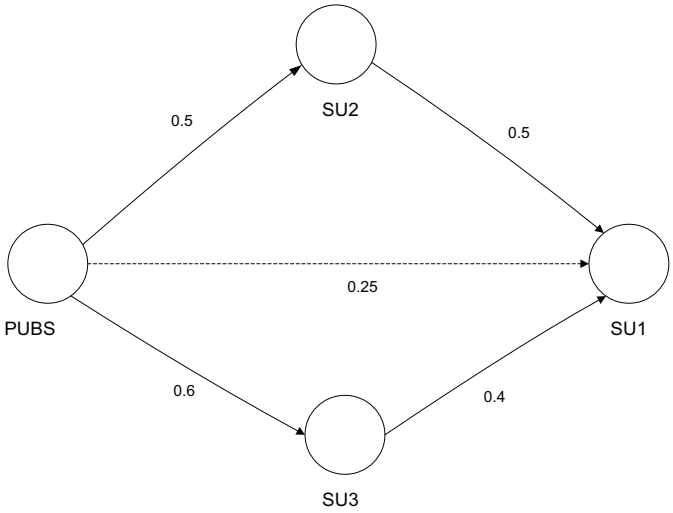

Figure 4. A new SU node within a reference trust relationship

4. AUTHENTICATING AND BIASING PROBLEM RESOLUTION

If a node is eligible to access the network resources, then, it will authenticated by the BS. This is done by having the SUBS compares the computed trust value, T, against the predefined threshold, $(T_{threshold})$. The candidate node is authenticated only if its trust value is greater than the required threshold, otherwise it request is rejected. On the other hand, the SUBS may forward the request to the PUBS, which also obtains the node's trust value and validates it against the authentication threshold. The node is authenticated only if it has trust value higher than the threshold. There are several advantages of adopting this mechanism. First, the network can support two levels of authentication. Second, certain nodes might be authenticated for certain resources but not for others, and finally, the threshold of authentication can be adjusted in order to relax or strict access based on how critical the application is.

Biasing may occur only at the SUBS, therefore, it is processed by the SUBS by asking the CA to provide the current candidate node's trust value, if there is one. The SUBS also obtain a trust recommended values from member nodes. The CA validates the candidate node's trust value it has through the public and private repositories, and communicates a validated one to the SUBS. The SUBS compares the computed received value from CA with the calculated one through members. If there is a difference, then the SUBS mark the candidate node's trust value as biased. SUBS then check the value communicated from members node before and after the biasing occurs. The SUBS then reports nodes that provide different trust values are 'malicious node' or 'biased by a malicious node'. This information is communicated to all of SUBS member nodes.

$$T_{dt} = \frac{\sum_{i=1}^{n} T_{A_i}}{\sum_{i=1}^{n} T_{A_i} + \sum_{i=1}^{n} (1 - T_{A_i})} = \frac{0.57 + 0.71 + 0.42}{(0.57 + 0.71 + 0.42) + (1 - 0.57) + (1 - 0.71) + (1 - 0.42)} = 0.56 \tag{6}$$

$$T_{reliable} = \frac{\sum_{i=1}^{n_{reliable}} T_{MR_i} \times T_{RC_i}}{n_{reliable}} = \frac{0.45 * 0.5 + 0.6 * 0.45 + 0.5 * 0.7}{3} = 0.28 \tag{7}$$

5. PERFORMANCE EVALUATION

We assume that none of the nodes is biased. The input parameters for the two networks are the number candidate nodes, the number of nodes in the network, and the threshold for trust. The first network acts

as secondary network and has 5 nodes. The second network acts as a primary network and also has 5 member nodes and one base station. We also assume that each has 3 criteria for trust. We also assume that a threshold trust value of 0.6 is initially used. Trust value calculation is conducted by members in the two networks using direct trust, and then communicated with the base station. The final trust value is them calculated by the base station and sent to the CA. The final trust value is then used to check for biasing make a decision about user authentication.

In this section we demonstrate authentication based on the trust value, where we consider three cases for node validation in both networks, in the first we address node authentication is granted in the secondary network, then node authentication is granted in the primary network, and finally, node authentication is denied. For authentication in the secondary network, we assume that node 2 is the candidate node in the secondary network, and that the rest of nodes will provide their trust recommendation about node 2 to the secondary network base station. It is also assumed that nodes are fair and not biased. We conducted simulation by generating 100 repetitive cases for the success and failure for each time period for three criteria, where trust value for the candidate node is assigned using equations 1 and 6. The trust values of the candidate node recommended from the four nodes in the secondary network for different time periods are shown in Table 2. Therefore, the average trust value of the candidate node for every criteria can be calculated. For instance for the first criteria it is equal to : $\frac{0.81+0.32+0.76+0.99}{4} = 0.72$. Then, the final trust value of the candidate node calculated from the using the three different criteria as :$\frac{0.72+0.67+0.45}{3} = 0.61$.

Table 2. Recommended trust value calculated from nodes in the secondary network using three criteria

Candidate Node	Node number in 'Network 1'	Criteria 1	Criteria 2	Criteria 3
4*Node 2	1	0.818	0.996	0.645
	3	0.321	0.045	0.998
	4	0.763	0.316	0.959
	5	0.996	0.855	0.487

In the next step, the computed trust value is compared with the trust threshold and the decision is made based on this comparison, as shown in Table 3. Since he computed final trust value of 0.61 is larger than the threshold value of 0.6, the SUBS authenticates the candidate node to accept its request to use the network resources or forwards its request to the secondary network as shown in Table 3.

Table 3. Authentication of candidate node in the secondary network

Candidate node	Trust Value of Candidate node			Final trust value	Threshold value	$\geq$ threshold ?	Decision
	Criteria 1	Criteria 2	Criteria 3		3*		
Node 2 Network 1' '	0.72	0.67	0.45	0.61	0.6	Yes	Request is authenticated or forwarded to 'Network 2'

For authentication in the primary network, we demonstrate an authentication request for a candidate node for the resources in the primary network. We assume that the primary network has five nodes and three criteria, where node 5 is assumed to be the candidate node. The member nodes of the primary network calculate the trust value for node 5 using direct trust from different time periods using three criteria as illustrated in Table 4. The average trust value of the candidate node for each criteria is calculated, for instance, for criteria 1 it is $\frac{0.59+0.95+0.76+0.93}{4} = 0.81$. The base station calculates the final trust value using :$\frac{0.81+0.55+0.77}{3} = 0.71$, which is then communicates it to the CA. This value is also used compared with the threshold of 0.6, and as a result, the candidate node is granted access to the primary network as illustrated in Table 5.

In this example we show request rejected case, where the same steps in the first case are performed, where node number 2 in the secondary network is the candidate node. Table 5 shows the final calculated trust value of 0.3 is less than the threshold value, therefore, the request is not authenticated in the secondary network. In other words, the candidate node is not considered valid and in its own network, therefore, the base station of the secondary network does not forward the request to access the primary network resources. Next, we consider the biased nodes case where a number of biased nodes takes part in the authentication process of certain nodes. This example will show how biasing is detected, and how the base station resolves this issue along with the CA. We assume that the secondary network has 5 nodes, and that node 3 is the candidate node. We will also assume

that some member nodes will intentionally assign biased trust values for the candidate node. Once biasing is detected, resolution is performed by the network as demonstrated.

Table 4. Recommended trust value calculated from nodes using three criteria in primary network

Candidate Node	Node number in 'Network 2'	Criteria 1	Criteria 2	Criteria 3
4*Node 5	1	0.599	0.996	0.645
	3	0.960	0.045	0.998
	4	0.765	0.316	0.959
	5	0.931	0.855	0.487

Table 5. Recommended trust value calculated from nodes using three criteria in primary and secondary networks

Candidate node	Trust Value of Candidate node			Final trust value	Threshold value 3*	≥ threshold ?	Decision
	Criteria 1	Criteria 2	Criteria 3				
Node 2 in 'Network 1'	0.81	0.55	0.77	0.71	0.6	Yes	Request is authenticated
Node 4 in 'Network 1'	0.21	0.33	0.47	0.33	0.6	No	Request is Declined

The candidate node's trust value is calculated by the member nodes in 'Network 1', where all member nodes are fair. For criteria 1, four nodes in 'Network 1' assign a trust value to the candidate node accordingly, as shown in Table 6 shows trust value for candidate node 3 before biasing. The final trust value for the candidate node as calculated by the base station in the secondary network is $\frac{0.8056+0.7842+0.5032}{3} = 0.6976$. This value is communicated to the CA, which stores it as the same for private value and public value for each node in the database before biasing. Assuming that member node 5 is biased, and that it will assign false trust values for the candidate node, the base station calculates the final trust value for node 3 in network 1 becomes 0.69, 0.93, and 0.57 for the three criteria with final value of 0.80, which is different from the trust value computed before biasing takes place. Once this trust value is communicated with the CA, it will be detected as biased due to large difference. In order to resolve this problem, the CA identifies all the trust values for all member nodes in both networks in the repository and forwards the information to the base station in the secondary network where biasing was initiated. This example shows how the biased value is detected in the secondary network. Once a biasing is detected, the case station checks for the trust value assigned by its nodes for all criteria as illustrated in Table 7, which shows that node 5 was biased with its trust assignment. Therefore, the secondary network base station communicates this information to all nodes in the network and excludes the biased node from further contributions in the trust calculation.

Table 6. Trust value calculated in secondary network using three criteria

Candidate Node	Node number in 'Network 1'	Criteria 1	Criteria 2	Criteria 3
4*Node 2	1	0.701	0.998	0.555
	2	0.983	0.787	0.582
	4	0.973	0.983	0.182
	5	0.584	0.376	0.725

Table 7. Trust value calculated for biasing detection in secondary network for different criteria

Criteria Criteria	Node number	Trust value before biasing	Trust value after biasing	Similar	Decision
4*1	Node 1	0.7016	0.7016	Yes	Not biased
	Node 2	0.9833	0.9833	Yes	Not biased
	Node 4	0.9737	0.9737	Yes	Not biased
	Node 5	0.5843	0.9999	No	Biased
4*2	Node 1	0.9982	0.9982	Yes	Not biased
	Node 2	0.7866	0.7866	Yes	Not biased
	Node 4	0.9833	0.9833	Yes	Not biased
	Node 5	0.3760	0.9999	No	Biased
4*3	Node 1	0.5554	0.5554	Yes	Not biased
	Node 2	0.5826	0.5826	Yes	Not biased
	Node 4	0.1822	0.1822	Yes	Not biased
	Node 5	0.7253	0.9999	No	Biased

6. CONCLUSION

In WPANs, certain untrustworthy nodes may have unauthorized access to certain resources due to high mobility of nodes. This affects the normal operation of the WPAN, as well as the ability to manipulate data being collected and is crucial if the data is either sensitive or used in mission critical decisions. In addition, any malicious activity by untrustworthy nodes can degrade the network performance and may cause malfunctioning of the whole WPAN. Since WPANs operate with sensors and devices that have resource limitations, a lightweight secure communication of nodes in WPANs is the main focus in this work as compared to other wireless paradigms, such as WiFi. This paper proposed a trust-based framework for authentication in WPAN that uses the concept of network slicing in order to virtually treat the WPAN as two separate entities: primary, and secondary networks. The method is based on obtaining an evaluation of trust for nodes that are willing to join the WPAN. A method is provided in order to maintain trust repository which is used to overcome biasing problem that arise from trust based authentication. The proposed trust based framework was shown to be lightweight and therefore can help in attaining secure communication among sensors and devices in WPAN.

REFERENCES

[1] L. Chen, S. Thombre, K. J"arvinen, E. S. Lohan, A. Al'en-Savikko, H. Lepp"akoski, M. Z. H. Bhuiyan, S. Bu-Pasha, G. N. Ferrara, S. Honkala, "Robustness, security and privacy in location-based services for future iot: A survey," *IEEE Access*, vol. 5, pp. 8956-8977, 2017.

[2] G. Sharma and S. Kalra, "A secure remote user authentication scheme for smart cities e-governance applications," *Journal of Reliable Intelligent Environments*, vol. 3, no. 3, pp. 177-188, 2017.

[3] W. Liu, K. Nakauchi, and Y. Shoji, "A neighbor-based probabilistic broadcast protocol for data dissemination in mobile iot networks," *IEEE Access*, vol. 6, pp. 12 260-12 268, 2018.

[4] A. Gawanmeh and A. Alomari, "Taxonomy analysis of security aspects in cyber physical systems applications," *IEEE International Conference on Communications Workshops*, pp. 1-6, 2018.

[5] B. Maram, J. Gnanasekar, G. Manogaran, and M. Balaanand, "Intelligent security algorithm for unicode data privacy and security in iot," *Service Oriented Computing and Applications*, vol. 13, no. 1, pp. 3-15, 2019.

[6] Y. Yang, L. Wu, G. Yin, L. Li, and H. Zhao, "A survey on security and privacy issues in internet-of-things," *IEEE Internet of Things Journal*, vol. 4, no. 5, pp. 1250-1258, 2017.

[7] J. JIANG and H. Guangjie, "Survey of trust management mechanism in wireless sensor network," *Netinfo Security*, vol. 20, no. 4, p. 12, 2020.

[8] M. E. Aminanto, R. Choi, H. C. Tanuwidjaja, P. D. Yoo, and K. Kim, "Deep abstraction and weighted feature selection for wi-fi impersonation detection," *IEEE Transactions on Information Forensics and Security*, vol. 13, no. 3, pp. 621–636, 2018.

[9] D. He, S. Zeadally, N. Kumar, and J.-H. Lee, "Anonymous authentication for wireless body area networks with provable security," *IEEE Systems Journal*, 2016.

[10] F. Rahman, M. E. Hoque, and S. I. Ahamed, "Anonpri: A secure anonymous private authentication protocol for rfid systems," *Information Sciences*, vol. 379, pp. 195-210, 2017.

[11] S. Mowla, N. Sinha, R. Ganiga, and N. P. Shetty, "Trust enhanced role based access control using genetic algorithm," *International Journal of Electrical and Computer Engineering*, vol. 8, no. 6, pp. 4724-4734, 2018.

[12] S. Chaudhary, A. Singh, and K. Chatterjee, "Wireless body sensor network (wbsn) security and privacy issues: A survey," *International Journal of Computational Intelligence and IoT*, vol. 2, no. 2, 2019.

[13] R. Lu, K. Heung, A. H. Lashkari, and A. A. Ghorbani, "A lightweight privacy-preserving data aggregation scheme for fog computing-enhanced iot," *IEEE Access*, vol. 5, pp. 3302-3312, 2017.

[14] K. Saleem, K. Zeb, A. Derhab, H. Abbas, J. Al-Muhtadi, M. A. Orgun, and A. Gawanmeh, "Survey on cybersecurity issues in wireless mesh networks based ehealthcare," *IEEE 18th International Conference on e-Health Networking, Applications and Services (Healthcom)*, pp. 1–7, 2016.

[15] V. Sharma, K. Lee, S. Kwon, J. Kim, H. Park, K. Yim, and S.-Y. Lee, "A consensus framework for reliability and mitigation of zero-day attacks in iot," *Security and Communication Networks*, vol. 2017, 2017.

[16] C. Deepa and B. Latha, "Hhsrp: A cluster based hybrid hierarchical secure routing protocol for wireless sensor networks," *Cluster Computing*, pp. 1-17, 2017.

[17] N.-N. Dao, Y. Kim, S. Jeong, M. Park, and S. Cho, "Achievable multi-security levels for lightweight iot-enabled devices in infrastructureless peer-aware communications," *IEEE Access*, vol. 5, pp. 26743-26753, 2017.
[18] Y. Wang, Z. Cai, X. Tong, Y. Gao, and G. Yin, "Truthful incentive mechanism with location privacy-preserving for mobile crowdsourcing systems," *Computer Networks*, vol. 135, pp. 32-43, 2018.
[19] I. Ullah, M. A. Shah, A. Wahid, A. Mehmood, and H. Song, "Esot: A new privacy model for preserving location privacy in internet of things," *Telecommunication Systems*, vol. 67, no. 4, pp. 553-575, 2018.
[20] S. Parvin, S. Han, B. Tian, and F. Hussain, "Trust-based authentication for secure communication in cognitive radio networks," *Int. Conference on Embedded and Ubiquitous Computing*, pp. 589-596, 2010.
[21] S. Parvin and F. K. Hussain, "Trust-based security for community-based cognitive radio networks," *IEEE 26th Int. Con. on Advanced Information Networking and Applications (AINA)*, pp. 518-525, 2012.
[22] S. Parvin, A. Gawanmeh, S. Venkatraman, A. Alwadi, and J. N. Al-Karaki, "Efficient lightweight mechanism for node authentication in wbsn," *Advances in Science and Engineering Technology International Conferences (ASET)*, pp. 1-6, 2018.
[23] A. Gawanmeh and Y. Iraqi, "Formal analysis of collision prevention of two wireless personal area networks," *Procedia Computer Science*, vol. 80, pp. 2362-2366, 2016.
[24] A. R. Dhakne and P. N. Chatur, "Tcnpr: Trust calculation based on nodes properties and recommendations for intrusion detection in wireless sensor network," *International Journal of Computer Science and Network Security (IJCSNS)*, vol. 16, no. 12, p. 1, 2016.
[25] Z. Ye, T. Wen, Z. Liu, X. Song, and C. Fu, "An efficient dynamic trust evaluation model for wireless sensor networks," *Journal of Sensors*, vol. 2017, 2017.

BIOGRAPHIES OF AUTHORS

Sazia Parvin is a Lecturer at Melbourne Polytechnic in Information Technology, Victoria. She is working as adjunct fellow as data and system security researcher at the School of Business, UNSW, Canberra. Her research interests include network security, trust management, cyber systems, cloud computing, big data analytics, system software and intelligent information systems. Her research is published in various top ranked publications. She has published over 27 research papers in her fields of interest as journals and international conferences. She is an Associate Editor for International Journal of Computer System Science and Engineering (IJCSSE) and International Journal of Engineering Intelligent Systems (IJEIS). She has achieved several prestigious Research Grants from Australia and South Korea. She is also the recipient of the 'Gold Medal' Bachelor of Computer Science and Engineering Award from Jahangirnagar University in 2004.

Amjad Gawanmeh (M'2011, Sm'2017) is an Associate Professor at the University of Dubai, UAE and affiliate Adjunct professor, Concordia University Montreal, Canada. He has two edited books, 3 book chapters, more than 25 peer reviewed Scopus indexed journal papers, and more than 50 peer reviewed conference papers. He was visiting scholar at Syracuse University, University of Quebec, and Concordia University. He is the Editor in Chief for the International Journal of Cyber-Physical Systems (IJCPS) IGI, an associate editor for IEEE Access Journal, and for Human-centric Computing and Information Sciences Journal, Springer. He acted as guest editor for several special issues. He is on the reviewer board for several journals in IEEE, Elsevier, Wiley, and many others. He acted as a member of the executive committee for IPCCC conference. He has co-chaired several conference workshops and special sessions organized in key conferences. He is an IEEE senior member.

Sitalakshmi Venkatraman is currently the Information Technology Lecturer and Discipline Leader for Business Information Systems at the School of Engineering, Construction & Design, Melbourne Polytechnic, Australia. She earned her PhD in Computer Science, with a doctoral thesis titled "Efficient Parallel Algorithms for Pattern Recognition", from National Institute of Industrial Engineering in 1993. In the past 25 years, Sita's work experience involves both industry and academics - developing turnkey projects for IT industry and teaching a variety of IT courses for tertiary institutions, in India, Singapore, New Zealand, and more recently in Australia since 2007.

Ali Alwadi is a graduated master student in electrical and computer engineering from Auckland University of Technology Auckland, New Zealand. He earned his MASC in engineering in 2017. Before that, he gradated from Yarmouk university, Irbid, Jordan in electrical and computer engineering. He worked in companies in the area of telecommunication and computer engineering in Jordan and New Zealand. He currently works as a technical Consultant for Bravura Solutions in New Zealand.

Jamal N. Al-Karaki (M'96, SM'12) received the Ph.D. degree from Iowa State University. He is an accomplished information security and technology expert with more than 15 years of versatile IT experience and expertise in corporate systems and network security architecture and management along with IT projects management, network and IT infrastructure design and implementation, and change management throughout the project life cycle in public and private sectors. He is the Co-Founder and Division Head of Information Security Engineering Technology with Abu Dhabi Polytechnic (ADPoly), Abu Dhabi, United Arab Emirates Before Joining ADPoly in 2012, he served as the Dean, the Department Head, the IT Manager, and the Principal Researcher in multinational environments. He has authored or co-authored over 50 published refereed technical articles in scholarly international journals and proceedings of international conferences.

Paul Yoo Paul is currently with the CSIS within Birkbeck College at the University of London and leading BIDA Data-Driven Cyber Security Laboratory. Prior to this, he held academic/research posts in Cranfield (Defence Academy of the UK), Sydney (USyd) and South Korea (KAIST). In his career, he has amassed more than 100 prestigious journal and conference publications, has been awarded more than US$ 2.5 million in project funding, and a number of prestigious international and national awards for his work in advanced data analytics, machine learning and secure systems research, notably IEEE Outstanding Leadership Award, Capital Markets CRC Award, Emirates Foundation Research Award, and the ICT Fund Award. Most recently, he won the prestigious Samsung award for research to protect IoT devices using machine-learning approach and Research England's Global Challenge Research Fund (GCRF) for research to protect global environment (e.g. marine resources) using edge intelligence techniques.