Development of FIGA: a Novel Trust-Based Algorithm for Securing Autonomous Interactions in WSN

Aderemi A. Atayero, Olusegun A. Ilori, and Michael O. Adedokun, *Member, IAENG*

***Abstract*—Attempts at securing wireless sensor networks (WSN) and making them more resilient and self-healing after attacks demand that services rendered by the network be secured on individual basis. The fact that a node is malfunctioning and/or has been compromised does not necessarily warrant its elimination from the network. Albeit, services such as routing, sensor readings, key distribution schemes, and others are handled in isolation and individually, due to the fact that an attack or malfunction may only be temporary. Moreover, an attack aimed at routing, or a particular application service does not invalidate nodes or the entire network. Consequently, Fuzzy Inference Gatekeeper Algorithm (FIGA); the algorithm presented in this paper proposes a piecemeal approach to WSN security. FIGA secures interactions in autonomous WSN by using a contextualized fuzzy inference system to combine trust scores from individual node interactions, reputation scores gotten from consultations and time dependent exponential trust scores. By so doing, we argue that autonomous WSNs can be better secured. We further illustrate the effectiveness of the FIGA against a simulated *Sybil* attack and discuss how the network recovers following such an attack.**

***Index Terms*— Algorithm, Sybil attack, Trust, WSN**

I. Introduction

In an increasingly connected and automated world, wireless sensor networks (WSN) provide a means of remotely sensing data, transferring sensed data, and in some cases actuation is done by WSN nodes [1]. WSN technology has potential for deployment in healthcare, military, environmental sensing, and home automation. However, it will be noted that many of the present and potential deployment scenarios of WSN require high security and resilience due to the fact that WSN technology can be insidiously employed to spy on people, manipulate decisions, or even, damage lives and property. Moreover, factors such as *adhoc* nature, mobility of connected nodes, limited computational resources, vulnerability to physical abuse or tampering, and limited (or unreliable) network connections make securing WSN a daunting task. Furthermore, unreachable and autonomous WSNs must be able to gracefully withstand attacks and recover thereafter.

A. WSN Background

WSN are by nature autonomous in their operations. In a sense, they provide a means of remotely gathering and aggregating data. However, the autonomous interactions this work refers to are the unsupervised operations carried out by sensor networks. Examples of interactions, which may be made autonomous are, propagation of trust across nodes, selection of trusted routes, identification of misbehaving nodes, and 'healing' after an attack. We discuss in subsequent subsections, the security requirements of autonomous WSNs and the requirements of self-healing networks.

B. Autonomous WSN Security Requirements

Machine-to-machine interactions between network-connected objects must authenticate, authorize, and monitor use of resources against abuse by users, and safely cooperate with one another. More specifically, failure must be graceful and recovery must be guaranteed. In the case of WSN which are essentially low-power devices with sensor(s), a processor, memory, power source, communication link (usually radio), and an actuator, autonomy in node and on the network is a required necessity. Security requirements of WSN are identified in [2]. In [3] self-organization and graceful degradation are respectively identified as security requirements of WSN security. These two security objectives are of particular importance in this research; the context-aware algorithm presented in this work aims to meet these requirements. FIGA is a gatekeeper algorithm, which approaches the problem of WSN security by the approach aiding individual nodes to make responsible decisions taking context of the interaction and the reputation of the other party into consideration.

C. Statement of Problem

In an increasingly interconnected world of the IoTs, the sheer number of connected objects and possible interactions between them make it difficult to externally control and supervise interactions between WSN nodes deployed in inaccessible locations. Furthermore, reliable WSN must evolve with fluctuations in energy, communication and ambient conditions. Therefore, one reliable way to safely link up the great number of autonomous interacting nodes entails: individual nodes acting responsibly and with discretion. Consequently, malicious or malfunctioning nodes are treated appropriately on an individual basis. In [4], the author identifies features of self-healing systems; elements relevant to self-healing WSN are: manifestation, duration,

Manuscript received July 07, 2015; revised August 19, 2015.

A. A. Atayero, O. A. Ilori and M. O. Adedokun are with the Department of Electrical and Information Engineering, Covenant University, 112233
A. A. Atayero, O. A. Ilori and M. O. Adedokun are with the Department of Electrical and Information Engineering, Covenant University, 112233 Ota, Nigeria (e-mail: atayero@covenantuniversity.edu.ng).

source, granularity, and detection of faults. As well as time constraints, system evolution, abstraction level, and behavioral predetermination. We argue that responsible self-configuring and self-healing nodes (in other words autonomous nodes) must incorporate some (if not all) of the features identified above. Therefore there exists a need for a scientific means of applying the elements of autonomous behaviour to WSN.

D. Aim and Objectives of Research

The aim of this work is to investigate the effect of divorcing authorization and authentication. Being authenticated should not automatically imply authorization to access all resources. The specific objectives are to demonstrate that:

1) the granularity of privilege, can better secure sensor interactions, while aiding graceful degradation and self-healing.
2) the popular SPIN protocol in WSNs has no direct means of intrusion detection; FIGA addresses this situation by appending a gateway algorithm, which responds differently to different services requests.
3) the ability of FIGA to mitigate on well-known WSN attack – the Sybil.

A Sybil attack, which occurs whenever a node assumes several identities with the objective of maliciously influencing the network, and modalities for mitigating such an attack with FIGA is taken as a case study.

E. Conceptual Contribution of the Research

This paper presents a means by which, node conduct can be quantified in a changing WSN with regard to context and node reputation on the network called FIGA. We apply fuzzy logic (policy), knowledge of the context, and reputation score of node to compute a weight value (trustworthiness), which informs the conduct of a node. More specifically, a collection of fuzzy rule bases defines policies governing interactions between nodes. The rules are selected in accordance to context. This is modeled by The Gatekeeper - a context-aware algorithm, which secures access to various resources (Fig 1). The algorithm presented in this work makes the following contributions:

1) The novel fuzzy inference based algorithm presented in this work combines reputation score and context-awareness in order to investigate its effects. In so doing, a systematic approach of combining both concepts is presented.
2) The context-aware algorithm presented is lightweight, hence suitable for WSN nodes, which, in some cases are 8-bit microcontrollers with <500 Bytes of RAM. We demonstrate how FIGA can be used to mitigate a Sybil attack.
3) Due to the great energy cost of radio transmission and serious energy constraints in WSN nodes, it is helpful for an algorithm like FIGA to evaluate the value of an interaction before a costly transmission operation is carried out.

II. LITERATURE REVIEW

In this section we present a review of works relating to security in WSN, trust and reputation/recommendation in WSN and fuzzy based trust systems, we also discuss context-awareness as it concerns WSN security. Subsequent sections are organized as follows: First we review works relating to trust and reputation based systems in general. Secondly, works relating to the use of trust-based systems in WSN are discussed. Thirdly, we present a review of fuzzy-based trust systems in recent literature and more specifically, in WSN and resource constrained embedded systems. Finally, we examine context-awareness in general and then subsequently as context specifically concerns WSNs.

A. Trust and Reputation Based Systems

In [5] taxonomy of trust-based systems in P2P systems is presented. Challenges presented by agent behaviour and system constraints are also discussed. The components of a reputation-based system, as identified, are shown in table I.

TABLE I
Trust and Reputation Based System Components [5]

Information Gathering	Scoring and Ranking	Response
Identity Scheme	Good vs. Bad Behaviour	Incentives
Information Sources	Quantity vs. Quality	Punishment
Information Aggregation	Time-dependence	
Stranger Policy	Selection Threshold	
	Peer Selection	

In this work, technical limitation of agents is identified as one of the constraints reputation systems. These limitations may include: bandwidth; processing capability, and in the case of WSN, energy limitations. The use of trust and reputation systems in distributed multi-agent systems (MAS), where agents have different and sometimes conflicting goals is discussed in [6].

We define Trust as measureable risk, while reputation is defined as information from third parties about a partner’s behaviour. The paper goes on to discuss multiple approaches to trust and reputation models namely: Socio-cognitive, Computational, and Reputational Models. An approach that

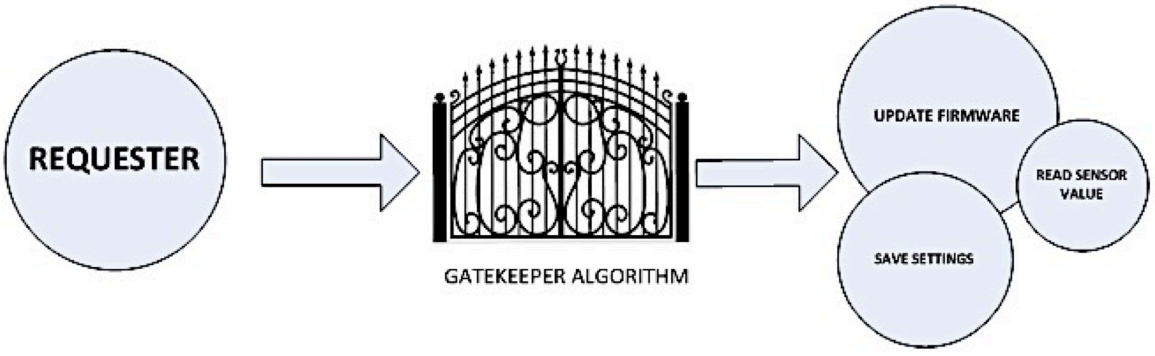


Fig 1. The Gatekeeper

might be most practical in autonomous interactions in WSN will be a hybrid of more than one or all of these approaches. However, due to the scope of this work and constraints of time, we have adopted a reputational model.

B. *Trust and Reputation Systems in WSN*

Trust and reputation based systems are applied in WSN, primarily in securing the network. Several works have been done in the area of quantifiable trust with applications, chiefly, in encryption key distribution and management. An extensive review of trust mechanisms in WSN, attack, and countermeasures is carried out in [7]. The authors in [8] present a mathematical algorithm, which uses mainly probability and statistics to adjudge reputation and then map this reputation into trust space in WSN. The authors argue that purely cryptographic methods are not sufficient to secure WSN nodes and networks. This is due to the fact that malicious nodes within the network may act to harm the network or other nodes. In this work bad behaviour is determined by intrusion detection (IDS) a well-established area of study [9]. Using a probabilistic value of certainty, a node maps reputation to trust. The computed level of trust is used to determine whether a node cooperates with another node.

Clustered WSN nodes with a compromised cluster head propagate the security problem in the network. In [10] a means of consistently electing well-behaved nodes as cluster heads is presented. The challenge with electing responsible cluster heads is that this approach can only work in a structured network. Not in one were nodes are consistently mobile and interactions may be spontaneous.

This research primarily uses fuzzy logic and inference to determine trustworthiness. However, fuzzy logic is by no means the only mechanism by which, trust can be determined. In [11] trust and reputation determination across different domains and using different methodologies are identified and discussed. Some of the methodologies identified are: Rating, Weighting, Probability, Bayesian network, Neural network, Game theory, Fuzzy logic, Swarm Intelligence, Directed and undirected graph (graph theory).

Heavy cryptanalysis has limited application in WSN. This is due to the fact that cryptography is computationally and energy expensive. Moreover, hardware accelerated cryptography is bound to raise the cost of WSN nodes. This research aims to keep computational load, energy, cost and network overhead as low as possible.

C. *Fuzzy Based Trust in Wireless Sensor Networks*

Trust is a fuzzy concept. It has elements of imprecision and vagueness; information leading to trust computation may arrive piecemeal, be unreliable or even contradictory. Fuzziness was formally introduced by Zadeh [12], and further extended and applied in several fields through the years [13]. Fuzzy trust is also being actively researched. [14] are a few areas where fuzzy trust is finding application ranging from e-commerce to grid computing. In [15], the authors use RFStrust - a fuzzy trust model- to secure mobile adhoc network. Their work is has some similarities to this research. For example, mobile adhoc networks (MANET) have similar limitations to WSN e.g. energy, computational and bandwidth limitations. Moreover, nodes might not have pervious knowledge of one another, and therefore no reputation history. Furthermore, trust values from other nodes are input to a fuzzy inference system in order to calculate the trustworthiness of a node. Fuzzy logic is used to estimate trust and control congestion on a WSN in [16]. Dud packets are injected and monitored. Fuzzy based inference is then used to identify and isolate selfish or malicious nodes on the network.

NBBTE (Node Behavioural Strategies Banding Belief Theory of the Trust Evaluation Algorithm), a novel algorithm is used in conjunction with modified evidence theory in [17]. Fuzzy sets are applied to evidence vectors. Ultimately, malicious nodes are identified by this means. Although, the work is not primarily based on fuzzy theory, fuzzy sets were used to graduate trust levels. Clearly, fuzzy logic is lightweight enough to be applicable in WSN domain. The FIGA algorithm, which we present in this work is fuzzy inference system; and while the gatekeeper algorithm adds slight computational load sensor nodes, the additional security is worth it.

D. *Context Awareness in WSNs*

According to [18],

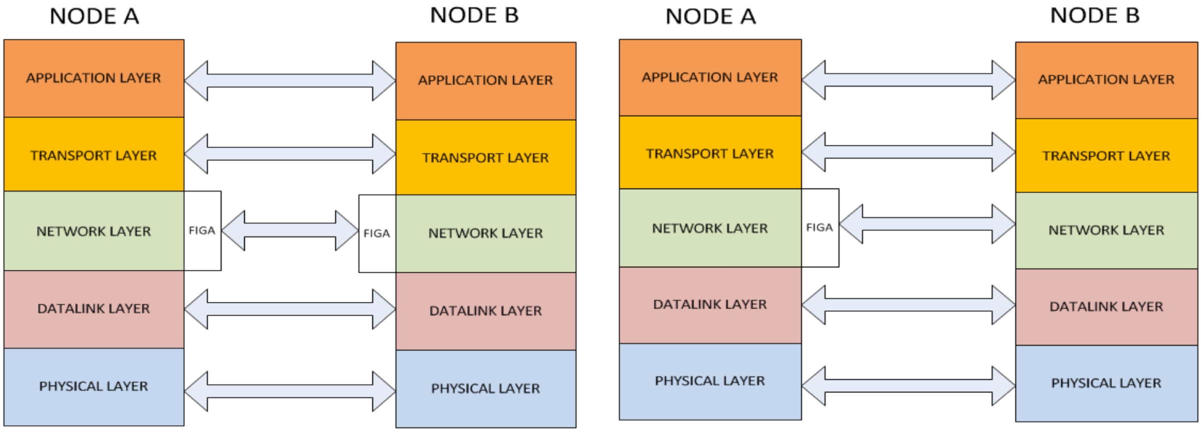
“Context-aware systems are able to adapt their operations to the current context without explicit user intervention and thus aim at increasing usability and effectiveness by taking environmental context into account”. Context-awareness thus enhances functionality, reliability and security of WSN. Two fault-tolerant, context-aware routing protocols (PEQ and CPEQ) are presented in [19]. Some security conflicts in WBAN are discussed in [20]. Finally, a survey of context-aware systems with emphasis on middleware and frameworks is presented in [18]. A layered framework comprising of sensors, middleware, and other resources; sensors may be real, virtual, or logical. Consequently, context awareness can be included as a layer (or sub-layer) in a layered architecture.

However, the approach presented by the authors is not applicable to WSNs due to the fact that it will introduce too much computational overhead. Consequently, we present a context-aware FIGA sub-layer, to secure interactions in WSN. Theoretically, FIGA can be any of the following layers: Application, network, and transport. However, in this paper we apply FIGA only in securing the network layer.

FIGA is loosely based on this architecture. However, implementing such a system completely on a WSN will be too cumbersome. Hence the gatekeeper algorithm, which is at the heart of this paper. It is really a context-aware rule engine, which stands between resources and a requesting node.

III. IMPLEMENTATION

In this section, we discuss the means by which FIGA was implemented. Firstly we give a general overview of the systems operation. Secondly we describe interactions within the context of WSN vis-à-vis security. Thirdly, the fuzzy inference system on which the entire system is centered is elaborated. Finally, the Sybil attack used to verify systems operation and how it is modeled is explained. The simulation was carried out using MATLAB and the fuzzy logic toolbox on a Windows PC.



(a) (b)

Fig 2. a) Nodes A and Node B with FIGA Protocol-Protocol interface; b) FIGA-equipped Node (A) with a non-FIGA equipped Node (B)

A. *General System Overview*

Networked entities are usually implemented in layered architectures. These layers do not necessarily represent any physical boundaries per se. Rather, the layers represent black boxes, which conceal the detailed inner operations of one layer to another layer. In the literatures [21], the following layers are identified as layers in WSN protocol stack: Physical, MAC (or datalink), Network (or routing), Transport, and Application layers. The fuzzy inference gatekeeper algorithm (FIGA) resides at the interface between protocol stacks resident on different nodes. However, FIGA equipped nodes can interact with nodes not equipped with the FIGA algorithm. An illustration of the FIGA interfaces between protocol levels is illustrated in Fig 2a. On the other hand, Fig 2b depicts a FIGA equipped node interfacing with a non-FIGA equipped node.

FIGA may be applied on the MAC layer to control flooding and spoofing, on the network layer, FIGA may be used to aid routing prioritization and mitigate routing attacks. Transport layers where present are prone to. This work focuses on the network layer. Typical services, which network layers provide to one another include host (or node) addressing, packet forwarding/routing, and path discovery are among the most common functions.

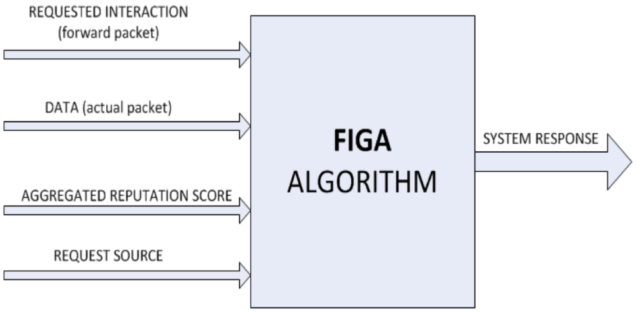


Fig 3. FIGA operational block diagram

The FIGA algorithm is the context aware gatekeeper, which, rests thinly on this interface. The services available on the network layer comprise the network layer interactions using the SPIN (Sensor Protocol for Information via Negotiation). SPIN as it were already provides a high-level data descriptor that describes the packet, which is being advertised, and since the SPIN does not enforce a metadata format, the particular deployment is free to create its own [22]. The context-atom described in [18] which, comprises of context-type, context-value, source of data, timestamp and confidence are represented as requested interaction, requested data, requesting source, timestamp, and reputation respectively.

Fig 3 depicts a block diagram of FIGA operation. Coming in to the system is a packet from another node, which requires forwarding. Attached to the packet is surrounding metadata. The surrounding metadata namely aggregated reputation score from other sources and from personal interaction with the requesting node and the packet source address, comprise the context of the interaction. FIGA is the fuzzy rule base, which puts all of these parameters together. It ought to be noted that the parameters are passed as metadata between nodes. The metadata communication employed in [22] and illustrated in Fig 4. The next section examines these input parameters formally and how they are quantified.

B. *FIGA Parameter Passing Handshake*

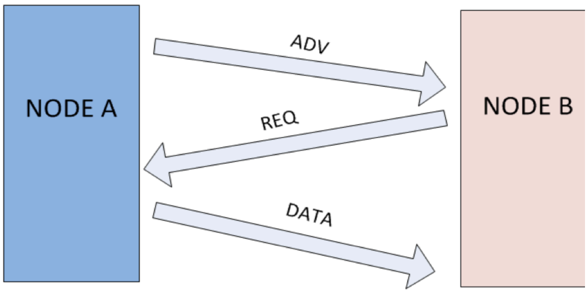


Fig 4. Spin-based 3-way handshake

Node A has a message to forward, it advertises its desire to forward the message using metadata (ADV). The neighboring node A respond back with a request for data (REQ), also metadata. Node A subsequently forwards the actual data packet to the respondent.

C. *Contextualized Interactions*

By the nature of protocols, only a limited number interaction types are possible between nodes on various layers. Put another way, communication protocols have a limited number of services available on each layer. For example, in the SPIN protocol used in this work, the handshake exchange comprises of ADV, REQ and the actual data exchange. On another layer such as the application layer, exchanges or interactions too are limited in number. Routing table exchanges, path discovery and node identification on the network layer have specified formats for exchanging them. Furthermore, WSN nodes being resource constrained have a smaller set of possible interactions. Popular application layer protocols used to exchange data in WSNs are Extensible Messaging Presence Protocol (XMPP) [23] and Constrained Object Application Protocol (CoAP) [24]. Both applications allow the end user to loosely define exchange details such as naming conventions and data content. However, for communication to be intelligible to the between nodes, formats have to be ultimately standardized in the end application.

Therefore, the most basic contextual elements comprises of the following:

- Name of source or destination: a means of identifying parties involved in the exchange. The name may otherwise be referred to as source or destination address
- Data content: the data payload to be exchanged
- Exchange Type (Optional): a parameter specifying the type of exchange.

Other kinds of context data may include timestamp, frequency of interaction, trust and reputation score.

Ultimately, the above description is an extension of the key-value model used in XML and other mark-up languages, which define sets of rules for specific exchanges.

D. *Growth and Decay of Trust*

Trust scores ranging between 1 and 0 are gotten from either personal interaction between nodes or by consultations. Mechanisms by which, trust is propagated are studied in [25]. This trust score is key contextual information in FIGA.

Trust in FIGA is derived through the number of interactions, which a node has with another. It grows and decays primarily with the passage of time. Trust scores between nodes decay exponentially with the passage of time. This decay occurs for two reasons. First, nodes that have not interacted in any particular context ought not to trust strange note wholeheartedly; rather, trust inherently grows with the passage of time. Secondly, the decay of trust serves as a means of 'forgetting' nodes such that nodes, which have not interacted for long periods of time begin to forget about such nodes. After a certain period of time, nodes, which have interacted, forget one another by so doing becoming strangers to one another.

The mechanism, which we have employed to model this decay and growth of trust is by the use of an exponential function

$$Tr = Te^{rt} \tag{1}$$

Tr is the instantaneous value of trust. T is the normalized value of trust (unity represents full trust and zero represents no trust). The exponential function is represented by e and r is the rate of decay and t is the time interval between interactions.

The decay and growth of trust is evaluated at regular intervals and is explained in more detail in the next section.

E. *Operational flow of the FIGA algorithm*

In this section, we describe the software flow of the FIGA algorithm resident on nodes. First, the interaction type is selected. This is implemented as a finite state machine (FSM). Secondly, the fuzzy rule base, which corresponds to the interaction type, is selected. Thirdly, the fuzzy inference algorithm is executed. Fourthly, the output of the fuzzy inference is defuzzyfied. Finally, the appropriate system response is applied.

F. *Decay and Growth of Trust Flow Chart*

The rate of decay r is set in accordance with the value of the interaction. As regards the choice of whether trust ought to grow (1) or decay (-1), depends on the following: a) successful completion of an interaction; b) decay happens if the converse occurs, and c) if a preset interaction span elapses, and no interaction occurs.

G. *Fuzzy Inference System*

The system, which aggregates reputation scores on a context-by-context basis, using a unique set of policies stored on the sensor node and fetched to infer system reactions. The fuzzy inference comprises of three fuzzy sets *i, r* and *e*. Each of the fuzzy sets comprises of three fuzzy subsets defined by trapezoidal membership functions illustrated in table II, where:

- i – trust gained from personal nodal interactions
- r – trust derived from neighbour node recommendations;
- e – reputation with time dependent growth and decay.

TABLE II: Fuzzy Rule Inequalities

Low	$\begin{cases} 0, & x \leq 0 \\ \frac{0.2 - x}{0.2 - 0.3}, & 0.2 \leq x \leq 0.3 \end{cases}$
Medium	$\begin{cases} \frac{x - 0.2}{0.4 - 0.2}, & 0.2 \leq x \leq 0.4 \\ 1, & 0.4 \leq x \leq 0.6 \\ \frac{x - 0.7}{0.4 - 0.7}, & 0.4 \leq x \leq 0.7 \end{cases}$
High	$\begin{cases} \frac{x - 0.7}{0.9 - 0.7}, & 0.7 \leq x \leq 0.9 \\ 1, & x \geq 0.9 \end{cases}$

H. *Modeling a Sybil Attack*

This approach towards using FIGA to tackle Sybil attacks bases on motivations for mounting Sybil attacks –the end which, the attacker hopes to accomplish. Consequently, by thwarting the motives, the attack is mitigated. In the literatures the following are identified as effects, which Sybil attacks have on WSN performance: ballot stuffing/ tampering with voting systems, preventing fair resource allocation, tampering with misbehaviour detection systems, attacks on trust and reputation systems

Sybil attacks are detrimental to geographic routing protocols, which require the exchange of location coordinates. By posing to have multiple identities, a single node can pretend to be in several locations at a single point in time.

IV. RESULTS AND DISCUSSION

In this section we discuss the effects FIGA has on actual autonomous WSN interactions. We show how trust grows between neighboring nodes with the passage of time and with increased numbers of interactions. We show quantitatively the minimum number of interaction, which is required to develop an adequate level of trust between nodes. Subsequently, we discuss how FIGA algorithm is used to counter a Sybil attack in a WSN.

A. *FIGA End-to-End Security*

FIGA secures the WSN in an end-to-end manner. In a WSN architected, upper layers namely: datalink, network, transport, and application layers may be secured by FIGA and are discussed shortly. However, the physical layer may yet benefit from FIGA by using the output of such inference in adjusting features identified in the literature, such as: duty cycle variation, mode change and priority messaging. Individual layer functions are discussed below:

Application layer – the chief aim of a malicious party will be to steal information they are not authorized to access. However, FIGA does not grant access to one and all as a typical passkey authenticated system does. Instead, access to different datasets requiring different levels of access is computed by FIGA. Transport layer – ensures reliability and provide congestion control. In WSN this layer is susceptible to attacks such as flooding, and desynchronization. Network layer – the network layer provides routing functions, it must be energy sensitive, network unique node identification, finding the most reliable path, which is a major concern of FIGA. Datalink layer – the datalink layer is primarily responsible for multiplexing data streams, error control. Datalinks may be rated according to overall energy efficiency, reliability and access delay.

A. *Trust between Neighbors*

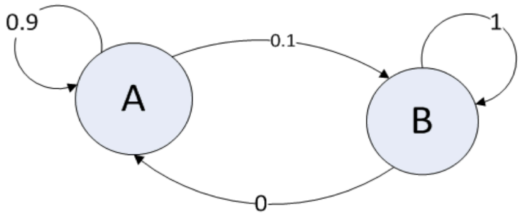


Fig 5. A Markov model of inter-nodal Trust

FIGA provides a means of combining individual knowledge of a node with collective knowledge from other nodes to rate datalink parameters. Fig 5 depicts a Markov model of the trust between neighbors used in FIGA.

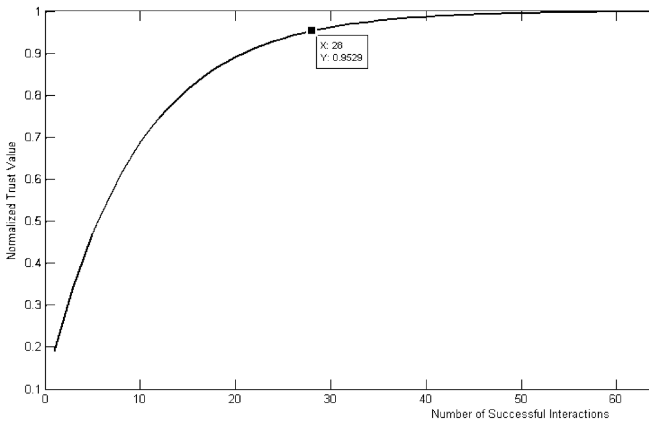


Fig. 6. Starting with 0.1 Trust level

In Fig 6, starting with 0.1 trust level, it takes 28 interactions to reach the 95th percentile when node B trusts node a far less. In Fig 7, the start trust level which node A has for node B is 0.4. It will be noted that it takes four fewer interactions (24) to reach the 95th percentile, because the trust values were more evenly distributed.

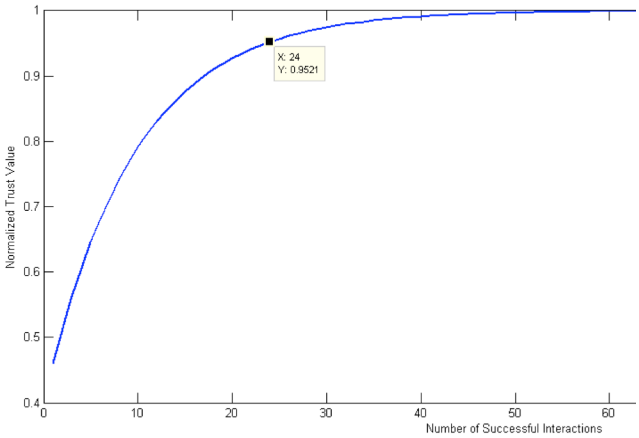


Fig. 7. Starting with 0.4 Trust level

B. *Mitigating a Sybil Attack*

First, it ought to be noted that a Sybil attack is never mounted for its own sake. They are usually carried out with a mind to gain undue access to resources, tamper with voting mechanisms, and/or tamper with routing paths among other reasons. Since each of these services are secured on an individual basis, FIGA, operating in a context-by-context mode renders the creation of such phantom nodes non-advantageous to the attacker. Even if reputations were assigned generically, the attacker scheme will be defeated since such nodes will have no reputations to speak of. FIGA is however more nuanced since reputation is assigned to services individually.

Under the proposed setup, when a trusted node suddenly creates new node with the aim of gaining undue advantage in a voting scheme or to crowd routing algorithm, with the aid of FIGA, such Sybil nodes have their votes carry less weight and their requests to have their data packets routed given less priority.

Although, some literatures examined in section 2 argue that Sybil attacks cannot be eliminated, the counter argument is that their deleterious effects on the network can be mitigated. With the use of context-aware varying fuzzy rules, we show that such nodes vary their policies to fit contexts. We show in the rest of this subsection that by varying policies to suit the context of voting and routing.

V. CONCLUSION

Autonomous WSNs are going to be inevitable in the near future. Improved wireless communications, better battery technology, cheaper and faster processor cores are going to make this possible. The Internet of Things requires large amounts of data sensing and actuation. WSN seems to be the technology best fitted for the large sensing requirements in an IoT environment; we have examined some IoT security concerns and likely solutions in [26]. However, in order to enable WSN technology to take its rightful place, they must be more resilient, self-healing an autonomous. FIGA provides just such a lightweight means of enabling such reliability and resiliency. Context-awareness as we have shown is a very important corollary in WSN operation and security. The FIGA, which has been prevented selects various policies appropriate to contexts. Another possible application area of FIGA is in securing WSN seat-locating technology e.g. SeatSense, which we have presented in [27].

A malignant party to a SeatSense WSN network may deduce lifestyle patterns and other private information from such a network. FIGA presents a means of securing just such a WSN- the malignant party will have no reputation to speak off on the network and therefore shall only be capable of assessing little information and carrying out little damage.

Furthermore, FIGA in collaboration with SPIN routing algorithm demonstrably mitigate the effects of Sybil attacks by weighing Sybil node request and responses less, thereby somewhat ostracizing them. FIGA may be applied in conjunction with the appropriate contextualized trust and reputation scores to every other WSN interaction. Ultimately, the proposed implementation for FIGA algorithm is with the APIs wrappers, which automatically exchange context data and return contextualized weighted values to the subroutines calling them.

This paper discussed multiple approaches to trust and reputation models namely: Socio-cognitive, Computational, and Reputational Models. And surmised that an approach that might be most practical in autonomous interactions in WSN will be a hybrid of more than one or all of these approaches. It however focused solely on the third model. An investigation into the socio-cognitive, computational and/or a hybrid of the models will be an interesting area of for future studies.

References

[1] Yick, J., Biswanath M., and Dipak G.. "Wireless sensor network survey." Computer networks 52, no.12 (2008): 2292-2330.

[2] Wang, Y., Garhan A., and Byrav Ramamurthy. "A survey of security issues in wireless sensor networks." (2006).

[3] Walters, John Paul, Zhengqiang Liang, Weisong Shi, and Vipin Chaudhary. "Wireless sensor network security: A survey." Security in distributed, grid, mobile, and pervasive computing 1 (2007): 367.

[4] Koopman, Philip. "Elements of the self-healing system problem space." (2003).

[5] Selcuk, Ali Aydin, Ersin Uzun, and Mark Reşat Pariente. "A reputation-based trust management system for P2P networks." In Cluster Computing and the Grid, 2004. CCGrid 2004. IEEE International Symposium on, pp. 251-258. IEEE, 2004..

[6] Keung, Sarah N. Lim Choi, and Nathan Griffiths. "Trust and reputation." InAgent-Based Service-Oriented Computing, pp. 189-224. Springer London, 2010.

[7] Yu, Yanli, Keqiu Li, Wanlei Zhou, and Ping Li. "Trust mechanisms in wireless sensor networks: Attack analysis and countermeasures." Journal of Network and Computer Applications 35, no. 3 (2012): 867-880.

[8] Reputation and Trust Mathematical Approach for Wireless Sensor Networks

[9] Axelsson, Stefan. Intrusion detection systems: A survey and taxonomy. Vol. 99. Technical report, 2000.

[10] Crosby, Garth V., and Niki Pissinou. "Cluster-based reputation and trust for wireless sensor networks." InConsumer Communications and Networking Conference. 2007.

[11] Momani, Mohammad, and Subhash Challa. "Survey of trust models in different network domains." arXiv preprint arXiv:1010.0168 (2010).

[12] Zadeh, Lotfi A. "Fuzzy sets." Information and control 8, no. 3 (1965): 338-353.

[13] Ross, Timothy J. Fuzzy logic with engineering applications. John Wiley & Sons, 2009.

[14] Song, Shanshan, Kai Hwang, and Mikin Macwan. "Fuzzy trust integration for security enforcement in grid computing." In Network and Parallel Computing, pp. 9-21. Springer Berlin Heidelberg, 2004.

[15] Luo, Junhai, Xue Liu, and Mingyu Fan. "A trust model based on fuzzy recommendation for mobile ad-hoc networks." Computer Networks 53, no. 14 (2009): 2396-2407.

[16] Zarei, Mani, Amir Masoud Rahmani, Avesta Sasan, and Mohammad Teshnehlab. "Fuzzy based trust estimation for congestion control in wireless sensor networks." In Intelligent Networking and Collaborative Systems, 2009. INCOS'09. International Conference on, pp. 233-236. IEEE, 2009.

[17] Feng, Renjian, Xiaofeng Xu, Xiang Zhou, and Jiangwen Wan. "A trust evaluation algorithm for wireless sensor networks based on node behaviors and ds evidence theory." Sensors 11, no. 2 (2011): 1345-1360.

[18] Baldauf, Matthias, Schahram Dustdar, and Florian Rosenberg. "A survey on context-aware systems." International Journal of Ad Hoc and Ubiquitous Computing 2, no. 4 (2007): 263-277.

[19] Boukerche, Azzedine, Richard Werner Nelem Pazzi, and Regina Borges Araujo. "Fault-tolerant wireless sensor network routing protocols for the supervision of context-aware physical environments." Journal of Parallel and Distributed Computing 66, no. 4 (2006): 586-599.

[20] Li, Ming, Wenjing Lou, and Kui Ren. "Data security and privacy in wireless body area networks."Wireless Communications, IEEE 17, no. 1 (2010): 51-58.

[21] Akyildiz, Ian F., and Ismail H. Kasimoglu. "Wireless sensor and actor networks: research challenges." Ad hoc networks 2, no. 4 (2004): 351-367.

[22] Heinzelman, Wendi Rabiner, Joanna Kulik, and Hari Balakrishnan. "Adaptive protocols for information dissemination in wireless sensor networks." InProceedings of the 5th annual ACM/IEEE international conference on Mobile computing and networking, pp. 174-185. ACM, 1999.

[23] Hornsby, Adrian, Petros Belimpasakis, and Irek Defee. "XMPP-based wireless sensor network and its integration into the extended home environment." InConsumer Electronics, 2009. ISCE'09. IEEE 13th International Symposium on, pp. 794-797. IEEE, 2009.

[24] Shelby, Zach, Klaus Hartke, and Carsten Bormann. "The constrained application protocol (CoAP)." (2014).

[25] Jøsang, Audun, Stephen Marsh, and Simon Pope. "Exploring different types of trust propagation." In Trust management, pp. 179-192. Springer Berlin Heidelberg, 2006.

[26] Atayero A.A., Ilori S.A, Adedokun M.O., (2015g), "Cloud Security and Internet of Things: Impact on Virtual Learning Environment", Proc., EDULEARN15 pp.3857-3863, 6th-8th July 2015 Barcelona (Spain).

[27] Atayero A.A., Ilori S.A., Adedokun M.O., (2015i), "Development of SeatSense: A WSN Based Seat Locating System", *Accepted*, (ICCSA), in IAENG WCECS 2015, 21st-23rd Oct 2015, San Francisco, USA.