TRUST MANAGEMENT FRAMEWORK IN WIRELESS SENSOR NETWORK: A SURVEY

Pranoti Dhairyashil Kale[1], R.M.Tugnayat[2]

[1]*Computer Department, BVCOEW, Pune, India*
[2]*Principal, SSACOE, Wardha, India*

Abstract

Trust can be calculated based on behavior of the node. Node misbehavior may be in terms of sending packet to wrong receiver, manipulating packet content, dropping packets while forwarding etc. Trust calculations depend upon input database either retrieved by node itself or retrieved by neighbor node. Input database refers interaction among the nodes that is behavior pattern and comparison of output of the normal routine response with standard behavior pattern. If there is variation in actual response against anticipated response that node need to be verified on the basis of meticulously crafted trust testimonial. Observing, comparing and analyzing variance with our previous experience may reduce energy consumption rather than starting from scratch every time.

Our contribution in this paper is to study state of the art research survey of existing trust calculation methodologies. Further Trust Management Framework explaining the phases of trust calculation, trust evaluation, trust outcome is proposed. This paper may be a good starting point for those who want to pursue research in trust management area of wireless sensor network.

Keywords—*Trust; decision making; Trust Management Framework; Trust evaluation; Trust calculation*

----------***----------

1. INTRODUCTION

Emerging domains in Wireless Sensor Network are energy conservation, data aggregation, topology control, routing protocol, duty cycle management, security management etc. All domains in Wireless Sensor Networks need decision making. Decision making in network involves set of possible inputs, possible outputs and mapping between them. Initially node will gather information either from its own experience or from its neighboring node. Based on that credence, trust is calculated and decisions may be taken consecutively.

Trust is any entity's belief in another entity may be based on its own experience or someone else experience so trust may be build individually or with feedback from neighbors. [1][2003] Dimitris Margaritis et al [2][2010] Mohammad Momani et al explained importance of study of "trust". For deriving trust value author suggested algorithms using different methodologies such as Rating, Weighting, Probability, Bayesian network, Neural network, Game theory, Fuzzy logic, Swarm intelligence etc. From observations about the network and applying different techniques like Bayesian effect, Game theory, Artificial intelligence etc decisions may be taken to define uncertainty in domain.

[3][2014] Guangjie Han et al, categorizes Trust models into node trust models and data trust models. Node trust models can be classified as Centralized trust models where base station or centralized authority calculates trust values of sensor nodes. In distributed node trust models, sensor nodes calculates trust values by themselves. In data trust model, trust is defined from vulnerability, eavesdropping, tampering data experiences while performing data sensing, processing and reporting are focused.

Next Section II discusses pros and cons of various models to be used in wireless sensor network. Section III includes fuzzy logic applications in wireless sensor network domain. Section IV describes existing work in trust management domain. Trust Management Framework is proposed in section V.

2. UNDERSTANDING PROS AND CONS OF MODELS TO BE USED IN WIRELESS SENSOR NETWORK

Bayesian network can handle uncertainty and involves cause-effect relationships. Every practical model is having cause and its corresponding effect. Cause effect pattern may be reused if associated environmental circumstances matches. In case if there is any uncertainty, it can be handled by theory of probability. Bayesian network is probabilistic model which represents random variables and dependencies among them. Bayesian model needs conditional as well as unconditional probability. It can predict probabilities for our proposed hypothesis but require lot of prior information. Major limitation of Bayesian network is for higher number of variables in large dataset, computation may be complicated.

Decision making may be modeled by game theory algorithm. It includes cooperation and conflict among player. Players may be neighbor node, sink, base station,

environmental factors. Studying the behavioral changes of faulty node, link affecting other nodes in the network may be game theory problem. Application wise different game theory methodologies can be suggested at each layer in protocol stack. Game theory can be applied whenever decision making depend on opponents strategies. Game theory may not be model based on exploration, surveillance, analysis.

[4][2006] Anders Walther et al applied artificial intelligence techniques to control the behavior of individual units. Strategies for each unit may be build by neural network or genetic algorithms, techniques under Artificial Intelligence domain. Neural network consists of input reflecting state of the problem domain having certain weight. Output is determined by an activation function where all the inputs are multiplied with their respective weights and then added together. Model is trained with learning data set, for verification of model validation data set is used and for determining user-friendliness of model testing set is used. Major limitation of neural network is trained data can not be upgraded whereas model need to be trained from scratch again. Neural network models may be more applicable in the study of brain, behavior pattern and respective computations.

Fuzzy Logic variables values may vary stepwise starting from 0 to maximum 1. It identifies input, output and its respective number of possible options. Uses various variables for possible options and derive procedural rule to perform the tasks. It uses descriptive language for input data so output may be expressed in percentage with respective to possible options.

To summarize for analysis of the network if objective approach is to be followed then Bayesian trust models may be applied. Subjective approach follows fuzzy logic to derive belief, uncertainty, confidence level etc. Subjective approach believes that evaluation of all kind of uncertainty may not be resolved by probability model. Game theory trust model may provide suggestions about the moves of opponent rather than a predictive tool for the behavior of nodes. Game theory is more applicable where bidirectional behavior is expected but wireless sensor network is one-way transmission.

Fuzzy logic seems to be one of the prominently used modelling technique in wireless sensor network. Next section focuses on existing work in wireless sensor network domain using fuzzy logic.

3. FUZZY LOGIC TECHNIQUE IN WIRELESS SENSOR NETWORK

Majority of researchers followed fuzzy logic techniques in existing different wireless sensor network domains. Fuzzy means repetitive division of problem till it is solvable. For each problem goals and objectives are defined. All input available is processed according to if-then rules based on the conditions in the process. Output decision is based on averaging and weighting the results from all the individual rules.

Generally input from sensors is suppose to be collected, sampled and based on local data decisions are derived from designed algorithms in the network. Rao and Georgeff in 1995 proposed an intelligent decision making theory “BDI model”. BDI signifies Belief Desire Intention. Beliefs are observations of the environment, the expected objectives or goals or tasks are Desires. Successful completion of desire including current belief set is chosen as Intention. As mentioned earlier collected data is converted to beliefs. First step followed is data gathering from deployed sensors. Next data aggregation and fusion will combine gathered data, extract features from data, local decisions are taken so overall analysis and interpreting output from the data.

[5][2007] S. Shen et al proposed belief generation algorithm by combining fuzzy reasoning with traditional BDI approaches for improving energy-awareness and utility. [6][2015] Vittorio P. Illiano et al focus more on operation related issues like sensor synchronization, network related issues like packet losses or delays. Sensors’ measurement process is affected by noise, faults, malicious data injections so characterized by a degree of uncertainty. Trustworthiness value is assigned by truster to each trustee having range from 0 to 1. Higher the matching between actual behavior of trustee and expected behavior, trustworthiness value will be more tending to 1. The nodes having very low trustworthiness value are called compromised nodes. This will help to classify outlying and non outlying measurements, author referred task of finding cause of the deviation as “diagnosis”. Distinguishing between cause of deviation whether it is fault or event of interest is challenging. Post diagnosis determining relevant course of action “attack” for the identified cause of the diagnosis is also important. Author proposed an algorithm for analyzing effect of above parameters on network performance.

Specifically for social network application [7][2007] Matthew J. Probst et al proposed algorithm for calculation of trust and confidence interval based on direct and indirect experiences about behavior of sensor node. Preconceived trust is decided by direct interaction with other individuals. Interaction may be in terms of sensing, routing and aggregation behavior of other nodes. Routing, aggregation through untrusted node is not permitted. Sensor node may be less trusted if perceived degradation in sensor accuracy is higher.

Fuzzy logic technique is applied in route discovery application. Decision among safest route is proposed by [8][2008] Tae Kyung Kim et al. For each route, for each hop author find evaluation value add all evaluation values out of all possible routes whichever path is having maximum trust aggregated value is chosen as safe path for packet transfer. This logic can differentiate between normal and abnormal sensors. Thus fuzzy logic technique is applied to trace out safest path among possible paths as well separate out abnormal sensors.

[9][2006] Leichun Wang et al proposed algorithm for establishing routes among the network. Each route initiates from gateway node and spreads in outward direction in multiple branches. Nodes with low energy, less bandwidth, high delay are avoided to get connected. Later nodes in a cluster delete multiple trees and thus connectivity among the network is established by choosing best path/s from multiple paths for data transmission. Author claim that proposed protocol performs well in saving energy and improving network lifetime.

Fuzzy logic techniques for improving Quality of Service is proposed by [10][2007] Luci Pirmez et al. It is a data dissemination protocol for selection of Quality of Service parameters based on input that is number of sensors, sink, task to be performed. Author claim that the algorithm reduces network resource consumption fulfilling application-specific requirements. Quality of Service parameters considered by author are delay, packet loss, energy, network lifetime. Algorithm can be updated in terms of adding Quality of Service parameters, network parameters, data dissemination protocols.

[11][2015] Wen Si et al proposed collaborative data gathering algorithm having some key parameters like residual energy level, number of neighbors, centrality degree and distance to the sink using fuzzy logic. The algorithm distribute equal workload among all sensor nodes. Correlation function in fuzzy theory is used for data aggregation among clusters. Proposed algorithm selects cluster head in distributed approach and improve the energy efficiency of the network.

Fuzzy logic applied in security domain of wireless sensor networks by [12][2007] Krontiris Ioannis et al. Author proposed lightweight scheme where nodes monitor their neighborhood and collaborate with their nearest neighbors, exchange the data with neighbors to decide about attack. Network-based Intrusion Detection System listen to network, captures network packets, examines individual packets and a node can overhear traffic passing from a neighboring node, nodes can mutually check network traffic. Intrusion Detection System can be used to detect black hole and selective forwarding attacks, producing very low false-negative and false-positive rates.

[13][2012] Dylan McDonald et al proposed Collaborative Tree-based Outlier Detection (CTOD) Framework algorithm with two modules communication module and confidence module. First, communication is minimized through an ad-hoc collaborative communication scheme which controls sensor behavior to increase overall visibility of individual streaming data sets. Second, an outlier detection algorithm is designed to identify the outlier candidate not identified by complete network. Third feature of framework is it can dynamically analyze network topology and create tree at execution time. CTOD Framework considers data distributions, network topologies, and methods of comparing data items to identify outliers. Algorithm can be applied for limited data set.

4. EXISTING WORK IN TRUST MANAGEMENT

Importance of trust is described by [14][2011] Luca Mottola et al. Identification of faulty sensor readings, temporarily isolating faulty node from network, finding actual reason for the identified fault will create trust in network. Algorithms should be proposed for observing, testing and validating behavior of applications developed. Author suggest WSN Community should define standards for defining benchmarks and metrics for evaluating system performance may be data collection, time synchronization. All these programmed algorithms should be tested and evaluated on actual nodes to take decisions in the network.

Decision making need input data set but whether individual data set is reliable, how much faith one should have on observations provided by input entities. Trust is confirmation or faith on input available. From raw input available extracting features is challenging task. Reputation is defined by individual trust instances.

[15][2011] Renjian Feng et al proposed trust factor is subjective and uncertain. It should be multiple valued logic may be comprising packet reception, packet sending, packet delivery, consistency and availability in packet transmission and reception etc. Trust value is based on evaluating node's observation on evaluated node. Trustworthiness levels is decided based on Fuzzy set theory and fuzzy functions.

Any node can collect and analyze experiences either by itself or from neighbors. [16][2010] Han Yu et al suggests from past behavior all positive and negative experiences can be collected either by itself or from neighboring nodes. From direct experience by node itself and indirect experience collected from neighbors, collectively aggregate experience is calculated. Behavior pattern of node is identified from aggregate experience. At individual level decision making is done by trust and reputation evaluation. From individual level decision making to system level decision making trust based reward punishment module and trust evidence dissemination modules are used by author.

Normally researchers consider data link, routing layer, transport layer algorithms in trust management domain. Whereas [17][2004] Elaine Shi et al proposed different perspective and proposed consideration of code attestation is very important along with traditional secure routing, authentication algorithm for outsiders, secure localization, link layer jamming that is congestion related issues etc. Code running on malicious node may be different from that running on legitimate node. Compromised node is the node on which a different version of code might be running. Code attestation concept is used for validating code running on each sensor node.

For trust calculations various approaches are used like encryption, decryption, generic model, ant colony concept, fuzzy logic are used by researchers.

4.1 Managerial architectural approaches [18][2010] Félix Gómez et al, [19][2007] Boukerch et al, [20][2010] Javier Lopez et al
4.2 Encryption Decryption [21][2012] Yanli et al. [22][2015] Juliano F. Kazienko et al, [23][2006] Crosby et al
4.3 Confident event detection [24][2010] Matthew Keally et al [25][2013] Min-Cheol Shin et al
4.4 Ant colony method [26][2011] Félix Gómez Mármol et al

4.1 Managerial Architectural Approach

Dedicated protocol stack for building trust are proposed by many authors. [18][2010] Félix Gómez et al proposed Trust and reputation model in wireless sensor network but author suggest need of standardization among research community. Model proposed by author should collect history and behavior should be ranked with score for that entity. Based on the score select the entity to interact for a particular transaction. Performance of transaction with the selected entity will decide rewards or punishments for that entity. Collection of history may be done directly by node or node may believe in feedback given by its neighbors or other node that is indirect experience.

An architectural approach is suggested by [19][2007] Boukerch et al proposed each network to be partitioned into clusters and each cluster is having backbone node as well as elected cluster head. Agent-based trust and reputation management scheme proposed by author includes Agent Launcher (AL), authority responsible for generating and launching TRAs into the network. Trust and Reputation Assessors (TRAs), mobile agent is generated by the AL and associated with every node and provide trust and reputation management service. Each node will hold a replica of the TRA's current version. Trust instruments (t-instruments) is segment of data issued by the local replica TRA of a node (issuer) to another node (issuee). Reputation certificates (r-certificates) is a segment of data issued by a replica TRA to its host. Thus verification of t and r certificate is done for trust and reputation management.

Checking reliability of indirect experience from neighboring node is very challenging. It may happen that in indirect experience any node may provide contradictory feedback. Related case studies are discussed by [20][2010] Javier Lopez et al in detail. Author describes various types of attack bad mouthing attack that is bad recommendation about honest node, On–off attack that is bad node behave sometimes in good way sometimes in bad way. Selective behavior attack that is node may have good recommendation from few nodes but it may damage certain nodes, Sybil attack and newcomer attack node can manipulate the recommendations and promote itself as a respected node. The above classification of attacks is based on internal node recommendations whereas it may be possible that external entities might attack.

4.2 Encryption Decryption

In data security, encryption and decryption is most popular tool for protecting data. External parameters attacking on network are explained by [21][2012] Yanli et al. Author suggested wireless sensor networks may suffer from external attacks such as eavesdrop on data, injecting fractional data, and manipulating the records for disturbing the normal working the network or internal attack such as invader breaking cryptography or authentication to capture sensor nodes. Confidentiality, Integrity, Authentication, Authorization, Availability, Freshness, Forward and backward secrecy, Self-organization, Auditing, Non-repudiation these characteristic are expected in each node.

A special secure key usage for encryption and decryption is proposed by [22][2015] Juliano F. Kazienko et al. To avoid tampering effect "SENSORLock" secure key is used for storage mechanism which protect all data stored in sensor memory. It stores all keys in memory, Sensor readings are encrypted with these keys the output is stored in crypt ographic module. The cryptographic module should be able to encrypt and decrypt keys. Key encryption and decryption may consume energy so applying these techniques in Wireless Sensor Network may not be feasible.

Cluster head perform data aggregation, data fusion, reporting to base station. Cluster head should not be a compromised node or malicious node. [23][2006] Crosby et al. proposed an algorithm for selection of cluster head so as to confirm that compromised or malicious node will not be selected as cluster head. Trust evaluation model is based on the three keys master, cluster and pairwise keys. Before any data packet operation all keys are verified thus compromised cluster head can be avoided. Encryption and decryption of keys consumes energy so this approach may not work for Wireless Sensor Network. Proposed algorithm do not consider any trust recommendation from neighbor node.

4.3 Confident Event Detection

Any event of interest detection by sensor node should be in time. Once occurred there should be assurance about detection. Algorithm need time for initialization, learning, event reporting. Trust can be created if networks designer is confident about happening of that event and correctly conveying it to the base station. [24][2010] Matthew Keally et al demonstrate the need for a new approach to confident event detection with reduced energy consumption. Our goal is to provide confident event detection at a critical point. Local Aggregation module aggregates observations from different sensor modalities. Cluster Generation identifies detection capability of a deployment which will suit the user requirement. Sentinel and Reinforcement Selection, clusters are selected that adapt the detection capability of a specific deployment to runtime observations. Author proposed "Watchdog" event detection framework to select group of sensors in such a way that event detection can be done confidently and save energy.

Different approach of grid based network is suggested by [25][2013] Min-Cheol Shin et al. Author proposed malicious node detection scheme using confidence level evaluation in a grid-based wireless sensor network. Inter-grid communications are employed, if necessary, to distinguish events from false alarms due to malicious nodes. Confidence levels of member nodes are updated to reflect their behavior in decision-making. The scheme is designed to identify malicious nodes even in the presence of relatively small event regions. Each grid is a cluster headed by cluster head. Cluster head have one communication channel for communicating within network other channel for communication among cluster heads. Sensor readings are categorized as "normal" readings and "unusual" readings. Malicious nodes can change the sensor readings arbitrarily. For detecting malicious nodes, confidence levels of sensor nodes considering trustworthiness boundaries.

4.4 Ant Colony Method

Behavior of ants for searching shortest path, path having less slope that is horizontal path, path with smoother surface, wider path logic is followed in ant colony algorithms. [26][2011] Félix Gómez Mármol et al proposed Bio-inspired Trust and Reputation Model for selecting trustworthy node in Wireless Sensor Networks. Model is based on ant colony system where ants build reputable path with certain conditions. Every node maintain pheromone traces for neighbors so that next node can discover and follow those routes. Since every node maintain its own pheromone traces for selecting a certain route as well heuristic values which is the inverse of the delay transmission time between two nodes make the network secure.

Trust management can not be in '1' or '0' format but it may have multiple states. Based on trust value job allocation that is sink aggregation or normal sensor node sensing function can be decided.

5. TRUST MANAGEMENT FRAMEWORK

Trust Management Framework is set of algorithms managing and supervising all trust functionalities. Trust is agile, dynamic entity. Reputation is submissive entity generated by many earlier instances of trust experiences.

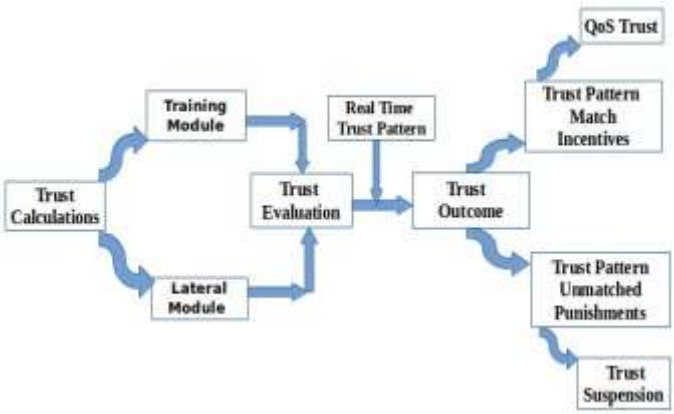

Fig 1 Proposed Trust Management Framework

Trust Calculation can be classified based on instance at which it is to be calculated. If trust is calculated initially post deployment of network it will be training module whereas if trust is updated it will be lateral module. Training Module follows observing the network, sending sample packets and checking response. Training module will believe more on recommendations or indirect experience. Lateral module will believe more on self or direct experiences.

Trust Calculation module should identify and select proper input which is Trust Evidence. Post selection of proper input sample, Trust Evaluation is benchmark allowing comparison of the prototype including set of illustrative samples and states.

Real time pattern may or may not match with Trust Evaluation trust pattern. If matched incentives or rewards will be added which will lead to Quality of Service trust. If real time pattern is not matching with earlier pattern, particular node sending that real time pattern may be removed that is suspended temporarily from network.

5. CONCLUSION

Decision making about trust needs input database either retrieved by node itself or retrieved by other node. This data is about interaction among the nodes that is behavior pattern. Comparing real time pattern with reference behavior pattern may lead to conclude whether it is normal routine response or changed response. If there is variation in actual response against anticipated response that node need to be verified on the basis of trust testimonial which are meticulously crafted tests. Observing, comparing and analyzing variance with our previous experience may reduce energy consumption rather than starting from scratch every time.

Our intuition suggest trust calculation frequency should vary according to network lifetime as trust is varying with time. For certain initial and final period of network lifetime frequency of trust calculation should be higher as initially trust is to be build and later in last phase of network lifetime network components failure may be higher. Trust with respective to network lifetime is like bell curve that is normal distribution. The probability that trust value is stable into certain interval incubate terminologies like confidence interval, reputation of the network.

"Variance" is the amount of risk the node is ready to take as behavior pattern is based on previous experience by the node itself or the recommendations. Based on trust values varying from 0 to 1 network will decide belief in every node. Trust Management Framework will help to detect the malicious nodes and eliminate them from the network temporarily till defect or fault is repaired.

ACKNOWLEDGEMENTS

We would like to thanks Dr. Vilas Thakre, Dr. Sangeeta Jadhav for their valuable suggestions and endless motivation.

REFERENCES

[1]. Dimitris Margaritis et al, "Learning Bayesian Network Model Structure from Data" Doctor of Philosophy Thesis School of Computer Science Carnegie Mellon University, May 2003.

[2]. Mohammad Momani et al, "Survey of Trust Models in Different Network Domains" arXiv preprint arXiv:1010.0168, 2010 - arxiv.org

[3]. Guangjie Han et al, "Management and applications of trust in Wireless Sensor Networks: A survey" www.elsevier.com/locate/jcss Journal of Computer and System Sciences 80 (2014) 602–617

[4]. Anders Walther et al, "AI for real-time strategy games" IT-University of Copenhagen Design, Communication and Media, June 2006.

[5]. S. Shen et al, "Fuzzy Decision Making through Energy-aware and Utility Agents within Wireless Sensor Networks" Artificial Intelligence Review, 27 (2-3): 165-187 2007

[6]. Vittorio P. Illiano et al, "Detecting Malicious Data Injections in Wireless Sensor Networks:A Survey" ACM Computing Surveys, Vol. 48, No. 2, Article 24, Publication date: October 2015.

[7]. Matthew J. Probst et al, "Statistical Trust Establishment in Wireless Sensor Networks" Proceedings of 13th International Conference on Parallel and Distributed Systems Dec 2007 Volume 01 Pages 1-8 IEEE Computer Society.

[8]. Tae Kyung Kim et al, " A Trust Model using Fuzzy Logic in Wireless Sensor Network" World Academy of Science, Engineering and Technology International Journal of Electrical, Computer, Energetic, Electronic and Communication Engineering Vol:2, No:6, 2008

[9]. Leichun Wang et al, "A Multiple-objective Fuzzy Decision Making Based Information-aware Routing Protocol for Wireless Sensor Networks", International Conference on Wireless Communication, Networking and Mobile Computing. WiCOM 2006

[10]. Luci Pirmez et al, " Applying fuzzy logic for decision-making on Wireless Sensor Networks" FUZZ-IEEE 2007 IEEE International Conference on fuzzy systems, London, UK, 23-26 July, *2007*

[11]. Wen Si et al, "A Collaborative Data Gathering Mechanism Based on Fuzzy Decision for Wireless Sensor Networks" Hindawi Publishing Corporation International Journal of Distributed Sensor Networks Volume 2015, Article ID 952428, 10 pages

[12]. Krontiris Ioannis et al, "Towards Intrusion Detection in Wireless Sensor Networks" Proceedings of the 13th European Wireless Conference, April 2007

[13]. Dylan McDonald et al, "CTOD: Collaborative Tree-Based Outlier Detection in Wireless Sensor Networks" MobiHoc ACM SIGMOBILE 2012

[14]. Luca Mottola et al, "Programming Wireless Sensor Networks: Fundamental Concepts and State of the Art" ACM Computing Surveys, Vol. 43, No. 3, Article 19, Publication date: April 2011.

[15]. Renjian Feng et al, "A Trust Evaluation Algorithm for Wireless Sensor Networks Based on Node Behaviors and D-S Evidence Theory" Sensors 2011, 11, 1345-1360; doi:10.3390/s110201345

[16]. Han Yu et al, "A Survey of Trust and Reputation Management Systems in Wireless Communications" Proceedings of the IEEE | Vol. 98, No. 10, October 2010

[17]. Elaine Shi et al, "Designing Secure Sensor Network" IEEE Wireless Communications December 2004

[18]. Félix Gómez et al, "Towards pre-standardization of trust and reputation models for distributed and heterogeneous systems" www.elsevier.com/locate/csi/Computer Standards & Interfaces 32 (2010) 185–196

[19]. A. Boukerch et al, " Trust-based security for wireless ad hoc and sensor networks" Science Direct Computer Communications 30 (2007) 2413–2427

[20]. Javier Lopez et al, "Trust management systems for wireless sensor networks: Best practices" Computer Communications 33 (2010) 1086–1093

[21]. Yanli Yu et al, "Trust mechanisms in wireless sensor networks: Attack analysis and counter measures" Journal of Network and Computer Applications, 2012 – Elsevier..

[22]. Juliano F. Kazienko et al, "On the Performance of a Secure Storage Mechanism for Key Distribution Architectures in Wireless Sensor Networks" Hindawi Publishing Corporation International Journal of Distributed Sensor Networks Volume 2015, Article ID 392495, 14 pages.

[23]. Crosby et al " A Framework for Trust-based Cluster Head Election in Wireless Sensor Networks" In Proceedings of Second IEEE Workshop on Dependability and Security in Sensor Networks and Systems, Columbia, MD, USA, April 2006; pp. 13-22.

[24]. Matthew Keally et al, "Watchdog: Confident Event Detection in Heterogeneous Sensor Networks" 16th IEEE Real-Time and Embedded Technology and Applications Symposium, RTAS 2010, Stockholm, Sweden, April 12-15, 2010

[25]. Min-Cheol Shin et al, "Malicious Node Detection Using Confidence Level Evaluation in a Grid-Based Wireless Sensor Network" http://dx.doi.org/10.4236/wsn.2013.53007 Published Online March 2013 (http://www.scirp.org/journal/wsn) Wireless Sensor Network, 2013, 5, 52-60

[26]. Félix Gómez Mármol et al, "Providing trust in wireless sensor networks using a bio-inspired technique" Springer Telecommun Syst (2011) 46: 163–180 DOI 10.1007/s11235-010-9281-7

[27]. Pedro B. Velloso et al "Trust Management in Mobile Ad Hoc Networks Using a Scalable Maturity-Based Model" IEEE Transaction on Network and Service Management, Vol. 7, No. 3, September 2010.