ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 7, July 2015

A Reliable Trust System for Clustered Wireless Sensor Network

Madhuri A. Giri [1], Poonam D. Lambhate [2]

P.G. Student, Department of Computer Engineering, J.S.C.O.E, Hadapsar, Pune, India [1]

Associate Professor, Department of Computer Engineering, J.S.C.O.E, Hadapsar, Pune, India [2]

ABSTRACT: In present day wireless sensor network (WSN) has become one of the most interesting networking technologies since it can be deployed without communication infrastructures. Wireless sensor networks is one in every of the outstanding computing network emerged worldwide as a result of its applications and options. A sensor network consists of an outsized variety of sensor nodes and a sink. The base station (BS) of WSN typically serves as a gateway to some other networks which provides a powerful data processing, storage centre, and an access point to the sensor nodes in its network. The system monitors the sensor nodes produces the actual false positives result nearly similar to the real time environment. A light-weight and dependable trust system (LDTS) projected for WSNs, use clustering algorithms. First, a light-weight trust decision-making theme is protected supported on the nodes' identities (roles) among the clustered WSNs that's acceptable for such WSNs as results of it facilitates energy-saving. As a result of cancelling feedback between cluster members (CMs) or between cluster heads (CHs), this approach can significantly will improve system efficiency whereas reduce the results of malicious nodes. A lot of significantly, lots of considerably CHs war massive amounts of knowledge data forwarding and communication jobs, a dependability-enhanced trust evaluating approach is outlined for co operations between CHs. This approach can effectively shrink effectively reduce networking consumption whereas malicious, selfish, and faulty CHs. Moreover, a self-adaptive weighted methodology square measure for trust aggregation at CH level. beyond these 3 area unit primarily used to solve whereas occurring the attacks(On-off attacks, Sybil Attack and new comer attack and conflicting behaviour attack) in between the sender and receiver.

KEYWORDS: cluster members, cluster head, lightweight trust decision-making scheme, dependability-enhanced trust evaluating approach, and self-adaptive weighted method.

I. INTRODUCTION

Wireless sensing element networks are composed of cheap, little and resource unnatural sensing element nodes, densely touch sensing fields that capture numerous styles of discourse data associated with their surroundings and create it offered to applications and services in alternative networks and application platforms. The safety and therefore the integrity of the info and therefore the communications between sensing element nodes are essential needs for finish applications to be reliable. The conventional read of security doesn't fulfil given the distinctive characteristics of sensing element networks that square measure prone to a spread of node misbehaviours. From compromised nodes acting as internal attackers to legitimate nodes that act egotistically, internal misbehaving nodes square measure a vulnerability that can't be tackled exploitation authentication and cryptography alone. This vulnerability, together with the cooperative nature of sensing element networks, imposes the necessity for assessing the trust relationships among the network nodes.

The notion of trust, as employed in totally different analysis areas like trusty computing, trusty platforms, trusty code and trust management, has received varied interpretations. Throughout this work, we tend to use the notion of trust because the quantified belief by a trust or with relevancy the ability, trust, security and responsibility of a trustee inside a fixed context''. we tend to study the matter of formulating analysis rules and policies, process trust proof, and

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 7, July 2015

testing and managing trust relationships, that square measure jointly spoken because the trust management drawback. The most objective of the trust management model projected during this work is that it ought to be applied uniformly throughout the device network. It ought to be ready to support, through correct configuration, from easy nodes that have terribly restricted role, process capabilities and will solely trust the nodes they are pre-configured to trust, to extremely adjusted nodes and gateways to alternative networks. The contribution of this paper may be a hybrid trust management model that mixes aspects from certificate based mostly and behaviour-based approaches on trust institution on common analysis metrics so as to permit for flexibility within the trust institution method, and allows the exploitation of pre-deployment data so as to regulate the supported trust characteristics for every node.

The resource efficiency and reliability of a trust system ought to without doubt be the foremost basic needs for any WSN (including clustered WSNs). However, existing trust systems created for clustered WSNs square measure incapable of satisfying these needs due to their high overhead and low reliability. A universal trust system designed for clustered WSNs for the synchronic action of resource potency and reliability remains lacking.

First, restricted work has targeted on the resource potency of clustered WSNs. A trust system ought to be light-weight to serve an oversized variety of resource-constrained nodes in terms of accuracy, convergence speed, and extra overhead [7], [8]. Supported an integrated comparison, variety of innovative works are developed for clustered WSNs, like GTMS [10], TCHEM [11], HTMP [12], ATRM [13]. However, most of those works did not think about the matter of resource constraints of nodes or used advanced algorithms to calculate nodes' trait. Implementing advanced trust analysis algorithms at every CM or CH is impossible. Though GTMS uses many novel mechanisms to boost the resource potency of clustered WSNs, this approach depends on a broadcast-based strategy to gather feedback among CMs, which needs a big quantity of resource and power.

II. RELATED WORK

A number of studies have proposed for WSNs such as [1] this paper describe the Networks together to create hundreds or thousands of low cost micro sensor nodes permits users to accurately monitor and predict the remote surroundings by expeditiously combining the data from the individual nodes. These networks require durable wireless communication protocols that are energy efficient and supply low latency. We develop and analyse low-energy adaptive clustering hierarchy (LEACH), a protocol design for small sensor networks that combines the ideas of energy-efficient cluster based routing and media access together with application specific data aggregation to attain good performance in terms of system period, deferred, and application-perceived quality. LEACH includes a new; administer cluster formation technique that permits self-organization of huge numbers of nodes, algorithms for adapting clusters and swapping cluster head positions to equally distribute the energy load among all the nodes, and techniques to authorize distributed signal process to avoid wasting communication resources. Our results shows that LEACH will improve system period by associate order of magnitude compared with general-purpose multi hop approaches.

III. PREDICTION AND DIAGNOSIS

When a network entity establishes trust in other network entities, it can predict the future reactions of others and diagnose their security properties. This prediction and diagnosis can solve or partially solve the following four important problems.

a) *Assistance in decision making to improve security and robustness:* With a prediction of the behaviours of other entities, a network entity can avoid collaborating with untrustworthy entities, which can greatly reduce the chance of being attacked. For example, a node can choose the most trustworthy route to deliver its packets in a MANET.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 7, July 2015

b) *Adaptation to risk, leading to flexible security solutions:* The prediction of nodes future behaviour directly determines the risk faced by the network. Given the risk, the network can adapt its operation accordingly. For example stronger security mechanisms should be employed when risk is high.

c) *Misbehaviour detection:* Trust evaluation leads to a natural security policy that network participants with low trust values should be investigated or eliminated. Thus, trust information can be used to detect misbehaving network entities.

d) *Quantitative assessment of system-level security properties:* With the assessment of trustworthiness of individual network entities, it is possible to evaluate the trustworthiness of the entire network. For example, the distribution of the trust values of network entities can be used to represent the healthiness of the network.

IV. TRUST METHODOLOGIES

This section provides a brief description about various trust methodologies which uses mathematical measures and models related to trust and reputation in wireless sensor networks [5].

A. *Bayesian Trust models*

This trust model is employed in [15]. It primarily consists of two directions: objective and subjective. In objective, trust analysis relies on the analysed information. In subjective, trust needs the amount of confidence throughout deciding operation [5]. To calculate trust, model will take either continuous trust or binary trust or each [4]. This trust system primarily depends on the records of the relevant behaviours of different nodes therefore; it will utilize the previous chance of an occurrence to update it with relevant behaviours of different nodes.

B. Subjective Logic Trust Model

This model is employed for analysing trust network and a Bayesian network that springs from dampster-shafer theory of proof. It's used for getting subjective beliefs regarding the degree of uncertainty truth propositions . To handle uncertainty of truth and anomaly detection, Subjective Logic Anomaly Detection (SLAD) Framework is employed. Supported the abnormal or anomalous information, SLAD conjointly uses Extended Subjective Logic primarily based algorithmic rule (ESLB). It deals with four tuple like belief, disbelief, uncertainty and base rate.

C. Entropy trust model

Entropy trust model is especially utilized in the sector of thermodynamics. Trust analysis in ad-hoc network makes use of Bayesian based trust propagation model and entropy based trust model. Entropy trust model is taken into account to be compatible with Bayesian theory model. Entropy principally deals with what proportion uncertainty is present in an exceedingly signal or random event.

D. Fuzzy trust model

Fuzzy logic provides AN approximate trust worth instead of actual trust worth. Fuzzy logic is going to be within the type of multi-valued logic that springs from fuzzy set theory. Fuzzy logic integrates a series of IF-THEN rules to resolve a problem within the system [5]. The necessary steps utilized in fuzzy logic are as follows

1. Initially, fuzzy sets and principles.
2. Initialize the input variables to the fuzzy engine.
3. Apply fuzzy rules to work out the output knowledge.
4. Appraise the results and eventually come the feedbacks to balanced criteria.

E. Game theory trust model

Trust management systems use scientific theory to avoid the uncooperative nodes within the network. This model mathematically captures the behaviour of nodes supported the behaviour of alternative nodes. Game model uses two modes of operation to notice the behaviour of nodes: the deterministic mode and also the random mode. In settled mode, the network is analysed. In random mode, a generic rule predicts the best responses in each game [4]. Game theory is not a prophetic tool to spot the behaviour of nodes rather it suggests however nodes need to behave [5]. Game theory performs bidirectional behaviour in sensing element network.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 7, July 2015

V. ESTABLISHMENT METHOD

Trust can be established in a centralized or distributed manner. Obviously, MANETs and sensor networks prefer distributed trust management, where each network entity maintains a trust manager.

a) *The trust record:* It is used to stores the information about trust relationships and associated trust values. A Trust relationship is always established between two parties for a enumeration. That is, one party trusts the other party to perform an action. In this work the first party is referred to as the subject and the second party as the factor. A notation: {*subject: agent, action*} is introduced to represent a trust relationship. For each trust relationship, one or multiple numerical values, referred to as trust values, describe the level of trustworthiness. There are two common ways to establish trust in computer networks. First, when the subject can directly observe the agent's behaviour, direct trust can be established. Second, when the subject receives recommendations from other entities about the agent, indirect trust can be established.

b) *Direct trust* is established through observations on whether the previous interactions between the subject and the agent are successful. The observation is often described by two variables: s, denoting the number of successful interactions, and f, denoting the number of failed interactions. For example, in the beta-function based method [2], the direct trust value is calculated as Recommendation trust is a special type of direct trust. It is for trust relationship *{subject: agent, making correct recommendations}*. When the subject can judge whether a recommendation is correct or not, the subject calculates the Recommendation trust from sr and fr values, where sr and fr are the number of good and bad Recommendations received from the agent, respectively. This judgment is often done by checking consistency between observations and recommendations, or among multiple recommendations. When using beta-function-based methods, the recommendation trust can be calculated as $\frac{s+1}{s+f+1}$.

c) *Indirect trust* can transit through third parties. For example, if A has established a recommendation trust relationship with B, and B has established a trust relationship with Y, A can trust Y to a certain degree if B tells A its trust opinion (i.e., recommendation) of Y. This phenomenon is called *trust propagation.* Indirect trust is established through trust propagation. Two key factors determine indirect trust. The first is when and from whom the subject can collect recommendations. For example, in a sensor network, a sensor may only get recommendations from its neighbours when there is a significant change in their trust records. This affects the number of available recommendations and the overhead of collecting recommendations. The second is to determine how to calculate indirect trust values based on recommendations. When node B establishes direct trust in node Y, and node A establishes recommendation trust in node B, A – B – Y is one recommendation path. One recommendation path can contain more than two hops, such as A – B1– B2 – … – Y, and there may be multiple recommendation paths, such as A – B1 – Y, A – B2– Y, …, and so on. Trust models determine how to calculate indirect trust between A and Y from trust propagation paths. There have been many trust models proposed for various applications.

VI. LDTS METHOD

It consists of following phases:

A. *Network Topology Model*

A trust-based framework for cluster-based WSNs in addition as a mechanism that reduces the chance of compromised or malicious nodes being selected (or elected) as cooperative nodes. A node within the clustered WSN model is known as a CH, or a CM.

B. *Lightweight Scheme for Trust Decision-Making*

LDTS facilitates trust decision-making supported a light-weight theme. By closely considering the identities of nodes in clustered WSNs, this theme reduces risk and improves system potency whereas resolution the trust analysis drawback once evidence is scant. A CM calculates the trust price of its neighbours supported two data sources: direct observations (or trust degree, DTD) and indirect feedback (or indirect trust degree, ITD). DTD is evaluated by the quantity of successful and unsuccessful interactions. During this work, interaction refers to the cooperation of two CMs.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 7, July 2015

All CMs communicate via a shared duplex wireless channel and operate within the promiscuous mode, that is, if node sends a message to CH via node, then node will hear whether or not node forwarded such message to CH, the destination.

C. Trust Relationships in LDTS

The trust relationship is mostly expressed as a particular quantitative worth. This worth will be a true variety between zero and one or a whole number between 0 and 100. During this work, we tend to remodel this value into an unsigned whole number within the interval between 0 and 10. Though presenting the trust values as a true variety or Associate in nursing whole number is also insignificant in ancient networks, this issue is of important importance for WSNs as a result of restricted memory moreover as transmission and reception power. This domain of trust values has the subsequent advantages.

D. Less memory overhead

An unsigned whole number between 0 and 10 solely desires four bits (0.5 bytes) of memory area, so saving save 50%memory area compared with trust values delineate as associate degree whole number between 0 and 100 (1 bytes) and 87.5% compared with trust values delineate as a true variety (4 bytes).

E. Less transmission overhead

Given that a smaller range of bits need transmission throughout the exchange of trust values between nodes, we tend to gain the good thing about less overhead of transmission and reception power.

F. Garnished attack

In such associate degree attack, malicious nodes behave well and badly or else with the aim of remaining unseen whereas inflicting harm. For example, fancy malicious nodes could suddenly conduct attacks as they accumulate higher trait.

G. Bad mouthing attack

As long as feedback is taken into account, malicious nodes will offer dishonest feedback to border sensible parties and/or boost trust values of malicious nodes. This attack, observed because the unhealthy mouthing attack, is that the most easy attack.

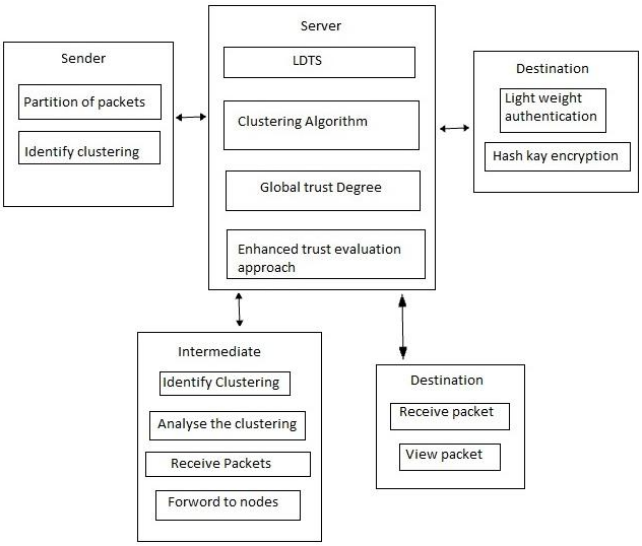

Fig 1: System Architecture

VII. EXPERIMENTAL RESULTS

The comparison results are shown in Fig. 2. With the increasing the number of CMs in a cluster, the CM-to-CM communication overhead of GTMS rapidly increased according to an exponential curve. However, the CM-to-CM communication overhead of LDTS slowly increased with the increasing number of CMs.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 7, July 2015

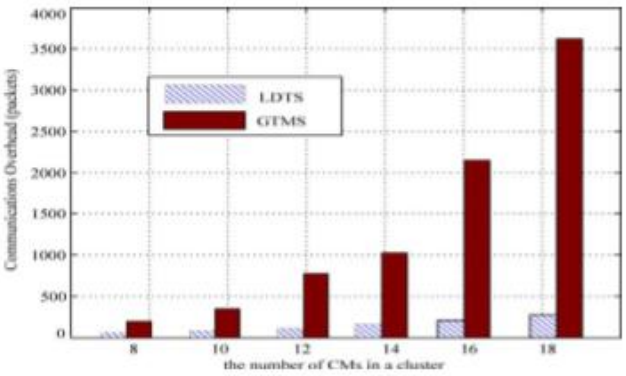

Fig 2: CM to CM communication overhead in a cluster.

Fig. 3 shows the comparison results of the CH-to-CH communication overhead between LDTS and GTMS. LDTS and GTMS have a relatively close network overhead as the network size increases, which indicates that both LDTS and GTMS are suitable for large-scale clustered WSNs.

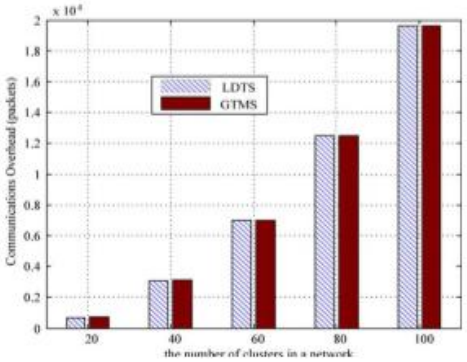

Fig 3: CH to CH communication overhead in a cluster.

Fig. 4 shows the comparison results of average storage overhead at each CM in a cluster. With the increasing number of CMs in a cluster, the average storage overhead of GTMS gradually increased according to a linear curve. However, the average storage overhead of LDTS was less than a third of that of GTMS and slowly increased with the increasing number of CMs.

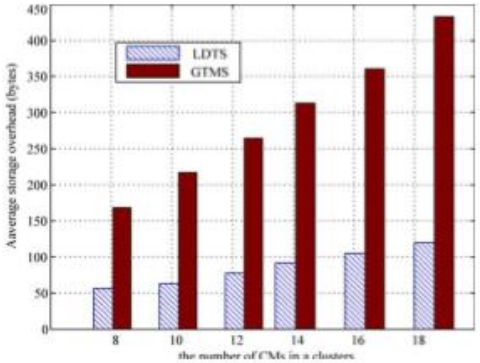

Fig 4: Average storage overhead at each CM in a cluster.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 7, July 2015

Fig. 5 shows the average storage overhead of the two trust systems at each CH in a WSN network having an equal size of clusters (10 nodes). We find that as the number of clusters increases in the network the GTMS introduces slightly less storage overhead compared with LDTS. Each CH has to maintain an additional table, which is used to store the feedback.

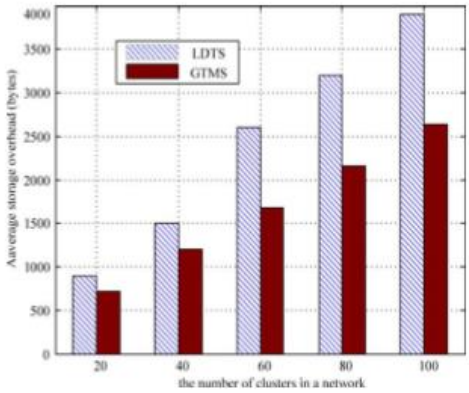

Fig 5: Average storage overhead at each CH in a cluster.

VIII. CONCLUSION

This paper proposed LDTS for clustered WSNs. Given the cancellation of feedback between nodes, LDTS can greatly improve system efficiency while reducing the effect of malicious nodes. By adopting a dependability-enhanced trust evaluating approach for cooperation's between CHs, LDTS can effectively detect and prevent malicious, selfish, and faulty CHs. Theory as well as simulation results show that LDTS demands less memory and communication overhead as compared with other typical trust systems and is more suitable for clustered WSNs. To overcome the problem of trust management against the attacks Such as conflicting behaviour attacks, Sybil attack and new comer attack ,on off attack and to solve the memory management problem.

REFERENCES

[1] S. Ganeriwal, L. K. Balzano, and M. B. Srivastava, "Reputation-based framework for high integrity sensor networks," ACM Trans. Sensor Netw., vol. 4, no. 3, pp. 1– 37, May 2008.

[2] Y. Sun, Z. Han, and K. J. R. Liu, "Defense of trust management vulnerabilities in distributed networks," IEEE Commun.Mag., vol. 46, no. 2, pp. 112–119, Feb. 2009.

[3] H. Yu, Z. Shen, C. Miao, C. Leung, and D. Niyato, "A survey of trust and reputation management systems in wireless communications," Proc. IEEE, vol. 98, no. 10, pp. 1752–1754, Oct. 2010.

[4] R. A. Shaikh, H. Jameel, B. J. d'Auriol, H. Lee, and S. Lee, "Group-based trust management scheme for clustered wireless sensor networks," IEEE Trans. Parallel Distrib. Syst., vol. 20, no. 11, pp. 1698–1712, Nov. 2009.

[5] F. Bao, I. Chen,M.Chang, and J. Cho, "Hierarchical trust management for wireless sensor networks and its applications to trust-based routing and intrusion detection," IEEE Trans. Netw. Service Manag., vol. 9,no. 2, pp. 169–183, Jun. 2012.

[6] G. Zhan, W. Shi, and J. Deng, "Design and implementation of TARF: A trust-aware routing framework for WSNs," IEEE Trans. Depend. Secure Comput., vol. 9, no. 2, pp. 184–197, Apr. 2012.

[7] E. Aivaloglou and S. Gritzalis, "Hybrid trust and reputation management for sensor networks," Wireless Netw., vol. 16, no. 5, pp. 1493–1510, Jul. 2010.

[8] Low Energy Adaptive Clustering Hierarchy with Deterministic Cluster-Head Selection M. J. Handy, M. Haase, D. Zimmermann Institute of Applied Microelectronics and Computer Science University of Rostock, Richard-Wagner-Str. 31, 18119 Rostock, Germany.R. A. Shaikh, H. Jameel, B. J. d'Auriol, H. Lee, and S. Lee,"Group-based trust management scheme for clustered wireless sensornetworks," IEEE Trans. Parallel Distrib. Syst., vol. 20, no. 11, pp.1698–1712, Nov. 2009.

[9] G. V. Crosby, N. Pissinou, and J. Gadze, "A framework for trust-based cluster head election in wireless sensor networks," in Proc. Second IEEEWorkshop on Dependability and Security in Sensor Networks and Systems, 2006, pp. 10–22.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 7, July 2015

[10] F. Bao, I. Chen,M.Chang, and J. Cho, "Hierarchical trust management for wireless sensor networks and its applications to trust-based routing and intrusion detection," IEEE Trans. Netw. Service Manag., vol. 9, no. 2, pp. 169–183, Jun. 2012.

[11] M. J. Handy, M. Haase, D. Timmermann Low Energy Adaptive Clustering Hierarchy with Deterministic Cluster-Head Selection M. J. Handy, M. Haase, D. Zimmermann Institute of Applied Microelectronics and Computer Science University of Rostock, RichardWagner-Str. 31, 18119 Rostock, Germany.

[12] R. A. Shaikh, H. Jameel, B. J. d'Auriol, H. Lee, and S. Lee,"Group-based trust management scheme for clustered wireless sensornetworks," IEEE Trans. Parallel Distrib. Syst., vol. 20, no. 11, pp.1698–1712, Nov. 2009.

[13] G. V. Crosby, N. Pissinou, and J. Gadze, "A framework for trust-based cluster head election in wireless sensor networks," in Proc. Second IEEEWorkshop on Dependability and Security in Sensor Networks and Systems, 2006, pp. 10–22.

[14] F. Bao, I. Chen,M.Chang, and J. Cho, "Hierarchical trust management for wireless sensor networks and its applications to trust-based routing and intrusion detection," IEEE Trans. Netw. Service Manag., vol. 9, no. 2, pp. 169–183, Jun. 2012.

[15] Quercia D, Hailes S, Capra L, B-trust: Bayesian trust framework for pervasive computing in: Trust management Proceedings of the fourth international conference, Trust 2006, Pisa, Italy, 2006.

[16] Mohammad Momani, Subhash Challa, Rami Alhmouz, "Bayesian Fusion Algorithm for Inferring Trust in Wireless Sensor Networks", Journal of Networks, Vol.5, No.7, 2010.