International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Impact Factor (2012): 3.358

Design of Secure, Reliable and Lightweight Communication in Trusted Wireless Sensor Network

Pradnya S. Kulkarni[1], Dr. Aarti Dixit[2]

[1]PVPIT, Bavdhan, Technology Department, Savitribai Phule University of Pune, Maharashtra, India

[2]Professor, PVPIT, Bavdhan, Technology Department, Savitribai Phule University of Pune, Maharashtra, India

Abstract: ***A sensor system will review our health, our home, the streets we follow, the workplace or the industry we work in or even the aircrafts we use, trying to improve our safety. Notwithstanding, the wireless sensor networks themselves are inclined to security attacks. The list of security attacks, in spite of the fact that officially exceptionally long, keeps on enlarging obstructing the development of these networks. The trust management schemes comprise of a powerful tool for the detection of unexpected node behaviors either malicious or faulty. In wireless sensor networks, sensor nodes in the region of interest must report the cognitive process to the sink by sensing, and this report will satisfies the report frequency necessary by the sink. Inside the domain of system security, we decipher the idea of trust as a connection among entities that take part in different conventions. Trust relations are focused around confirmation made by the past connections of substances inside a convention. In wireless sensor network the resource efficiency and reliability of a trust system are the most basic supplies. Due to the low reliability and high overhead the developed existing trust systems for wireless sensor networks are unable of satisfying these supplies. Therefore there is need to propose a lightweight and reliable trust system which can efficiently decrease the networking consumption while malicious, selfish and faulty cluster heads and also exceeds the limitations of traditional weighting methods for trust factors in which weights are allocated subjectively and also insist less communication overhead and memory.***

Keywords: Wireless sensor network, trust management, reputation, trust model, self-adaptivity.

1. Introduction

Wireless sensor systems propose conceivably helpful arrangements for different applications including atmosphere and temperature observing, freeway traffic analyzing, individuals' heart rates sensing, and numerous other military applications. A real feature of these systems is that sensor nodes in systems help one another by passing information, in network process and control packets starting with one node then onto the next. It is regularly termed an infrastructure-less, self-organized, or spontaneous system.

Trust management is major to recognize pernicious, selfish and compromised nodes which have been validated. It has been broadly contemplated in numerous network situations, for example, peer-to-peer network, peer and pervasive processing et cetera. Be that as it may, in all actuality, sensor nodes have constrained assets and other extraordinary characters, which make trust management for WSNs more critical and testing. Up to the present, explore on the trust management components of WSNs have mainly focused on nodes' trust assessment to upgrade the security and power. The reasonable applications of this strategy incorporate the course, information incorporation and cluster head vote.

Clustering algorithms can effectively improve the network throughput and scalability for wireless sensor network like EEHC [8], HEED [9], LEACH [4], and EC. The nodes are grouped into the cluster with the help of clustering algorithm and within each cluster the node which have high computing power and energy selected as a cluster head (CH).Typically the nodes closer to the base station will be vigorously loaded. Trust foundation in a grouped environment is of incredible criticalness. Trust is the desire of one element about the activities of an alternate. A trust framework empowers a CH to recognize faulty or malicious nodes inside a group, guides the selection of trusted routing nodes through which a cluster member (CM) can send information to the CH. Amid inter cluster communication, a trust framework additionally helps in the selection of trusted routing gateway nodes or other trusted CHs through which the sender node will forward information to the base station (BS).

A WSN contains battery-power sensor nodes with greatly restricted handling abilities. With a thin radio communication range, a sensor node remotely sends messages to a base station through a multihop path. The asset effectiveness and reliability of a trust framework are the most basic necessities for WSNs. Then again, existing trust frameworks created for clustered WSNs are unequipped for fulfilling these necessities due to their high overhead and low reliability.

Additionally, implementing complex trust assessment calculations at every CM or CH is not practical. In existing trust mechanisms, trust management system gather remote feedback and then the criticisms from all the nodes are aggregated to get the worldwide notoriety which can be utilized to assess the global trust degree (GTD) of this node. Because of the broadcast nature of the WSN environment, it contains a substantial number of undependable or malicious nodes. Criticism from these undependable nodes may bring about the incorrect evaluation of feedback. So a trust system ought to be profoundly reliable as far as giving administration in an open WSN environment.

Licensed Under Creative Commons Attribution CC BY

2. Trusted WSN

Trust in WSN systems assumes a critical part in building the system and making the expansion and/or cancellation of sensor nodes from a network, because of the development of the network, or the substitution of falling flat and temperamental nodes exceptionally smooth and transparent. The creation, operation, management and survival of a WSN are reliant upon the helpful and trusting nature of its nodes; consequently the trust establishment between nodes is an absolute necessity. In any case, utilizing the conventional apparatuses, for example, cryptographic tools to create trust confirmation and make trust and traditional protocols to trade and disperse keys is unrealistic in a WSN, because of the asset restrictions of sensor nodes by L. Eschenaue[16]. Hence, new imaginative methods to secure communication and dispersion of trust values between nodes are required. Trust in WSNs, has been examined delicately by flow analysts regardless is an open and testing field.

On Trust Models and Trust Evaluation Metrics for Ad Hoc Networks (George Theodorakopoulos and John S. Baras, 2006) [1] focus on the trust evaluation evidence in ad hoc networks. Trust evidence may be uncertain and incomplete due to the ad hoc networks dynamic nature. This scheme is completely focused around data starting at the clients of the system. No unified framework is needed, despite the fact that the vicinity of one can positively be used. Additionally, clients require not have individual, immediate experience with each other client in the system so as to figure an assumption about them. They can build their conclusion in light of used proof gave by moderate nodes, accordingly profiting from other nodes' encounters.

An Application-Specific Protocol Architecture for Wireless Micro sensor Networks by Heinzelman et al. (2002) [4] create and dissect low-energy adaptive clustering hierarchy(LEACH), a protocol construction modeling for micro sensor systems that consolidates the thoughts of energy-efficient cluster-based routing and media access together with application-specific data aggregation to attain great execution regarding framework lifetime, idleness, what's more application-saw quality. LEACH incorporates another, distributed cluster development procedure that empowers relationship toward self-organizations of extensive quantities of nodes, algorithms for adapting clusters also turning cluster head positions to equitably distribute the energy load among all the nodes, and methods to empower dispersed sign handling to spare communication assets.

In EEHC: Energy efficient heterogeneous clustered scheme for wireless sensor networks by Kumar et al. (2009) [8] proposed an energy efficient heterogeneous cluster plan for wireless sensor networks. The energy efficiency furthermore simplicity of organization makes EEHC an attractive and hearty protocol for wireless sensor networks. Keeping in mind the end goal to enhance the lifetime and execution of the system network, this paper covers the weighted likelihood of the selection of cluster heads. Reproductions results demonstrate that EEHC has expanded the lifetime of the system by 10% as contrasted and LEACH in the vicinity of same setting of capable nodes in a network. Henceforth, the execution of the proposed framework is better regarding dependability and lifetime.

O. Younis and S. Fahmy (2004) [9] present a convention, HEED (Hybrid Energy-Efficient Distributed grouping), that intermittently chooses cluster heads as per a hybrid of the node residual energy and an auxiliary parameter, for example, node nearness to its neighbors or node degree. Regard ends in O(1) cycle, causes low message overhead, and accomplishes genuinely uniform cluster head circulation over the system.

In LEAP: Efficient Security Mechanisms for Large Scale Distributed Sensor Networks by Zhu et al. (2003) [11] depict LEAP (Localized Encryption and Authentication Convention), a key management protocol for sensor networks that is intended to backing in-network processing, while in the meantime confining the security effect of a node compromise to the quick system neighborhood of the compromise node. The outline of the protocol is motivated by the perception that distinctive sorts of messages traded between sensor nodes have diverse security prerequisites, and that a solitary keying component is most certainly not suitable for gathering these diverse security necessities.

In SPINS: Security Protocols for Sensor Networks by Perrig et al. (2002) [12] present a set of security building blocks optimized for resource constrained environments and wireless communication. SPINS has two secure building blocks: SNEP and _TESLA. SNEP provides the Data confidentiality, two-party data authentication, and data freshness important baseline security primitives.

TRECON: A Trust-Based Economic Framework for Efficient Internet Routing (Zhengqiang Liang and Weisong Shi, 2010) [5] assemble a trust-based financial skeleton called TRECON to address these open issues in Internet routing. The oddity of TRECON is joining a adaptively personalized trust model with a monetary methodology to give autonomous trust-based routing among Sps. TRECON gives adaptable strategy help in light of the trust-based economic mechanisms so that independent associations with differed diversions and streamlining criteria can be easily incorporated together to attain better adaptiveness also organization toward self-management.

In Reputation-based Framework for High Integrity Sensor Networks by Ganeriwal et al. (2008) [6] displayed a summed up and unified methodology for giving data authentication by displaying it as an issue of creating a cluster of dependable sensor nodes. We created a Reputation-based Framework for Sensor Networks (RFSN), where every sensor node maintains reputation for different nodes. This reputation can be utilized as an intrinsic viewpoint as a part of foreseeing the future behavior of the nodes, subsequently permitting the identification of getting rowdy nodes. RFSN coordinates apparatuses from facts and choice hypothesis into a far reaching, appropriated and totally scalable framework.

In Information Theoretic Framework of Trust Modelingand Evaluation for Ad Hoc Networks by Han et al. (2006) [7] present a data theoretic schema for reliability assessment in

Licensed Under Creative Commons Attribution CC BY

distributed networks. Four adages are produced to address the importance of trust and create trust relationship through outsiders. Taking into account these aphorisms, the level of reliability can be quantitatively decided taking into observation and through proliferation. Two models that represent linking and multipath spread of trust are produced.

3. Trust Management System

Trust is a critical variable in the choice making procedures of any system where instability is a component. Management System: if a component of the system knows ahead of time the real conduct of their accomplices (e.g. malicious, faulty, and collaborative), it can settle on an impeccable choice. All the components of the network work towards the same objective, and they have not reason or the will to carry on selfishly. On the other hand, a sensor node does not have data with respect to others that will permit it to know ahead of time how a transacting accomplice is going to act. Thusly, there is some data asymmetry that the node must arrangement with. At the point when a sensor node picks an accomplice to team up with, such accomplice should be fair and completely synergistic. Sensor systems can endure the attack of noxious nodes or the presence of flawed nodes. As a result, vulnerability in sensor networks is an issue that must be managed a Wireless Sensor Network must be ready to design itself amid its lifetime in vicinity of exceptional occasions.

In Group-Based Trust Management Scheme for Clustered Wireless Sensor Networks by Shaikh et al. (2009) [10] propose another lightweight group based trust management system (GTMS) for wireless sensor networks, which utilizes clustering. This methodology decreases the expense of trust assessment. Additionally, hypothetical and simulation results demonstrate that this plan requests less memory, energy, and communication overheads as contrasted with the current condition state-of-the-art trust management scheme and it is more suitable for substantial scale sensor networks. Moreover, GTMS additionally empowers us to recognize and avoid malicious, faulty and selfish nodes.

In Hierarchical Trust Management for Wireless Sensor Networks and its Applications to Trust-Based Routing and Intrusion Detection by Bao et al. (2012) [2] proposed a hierarchical dynamic trust management protocol for cluster-based wireless sensor networks, considering two parts of reliability, to be specific, social trust furthermore Qos trust. We created a likelihood model using stochastic Petri nets methods to dissect the convention execution; also accepted subjective trust against target trust got focused around ground truth node status.

Crosby et al. [13] proposed TCHEM, a distributed trust-based framework and a mechanism for the vote of trustworthy cluster heads. This mechanism reduces the likelihood of compromised or malicious nodes from being selected as cluster heads. TCHEM does not cover trust in detail, since numerous key issues of trust management are not introduced.

Boukerche*et al.* [14] proposed ATRM, a novel agent based trust and reputation management scheme (ATRM) for wireless sensor networks. Trust and reputation is suggested as an effective security mechanism for open environments such as the Internet, and considerable research has been done on modeling and managing trust and reputation. Using the trust and reputation management scheme to secure wireless sensor networks (WSNs) requires paying close attention to the incurred bandwidth and delay overhead, which have been focused by most research works. The objective of the scheme is to manage trust and reputation locally with minimal over head in terms of extra messages and time delay. ATRM assumes that mobile agents are resilient against malicious nodes that try to steal or modify information such agents carry.

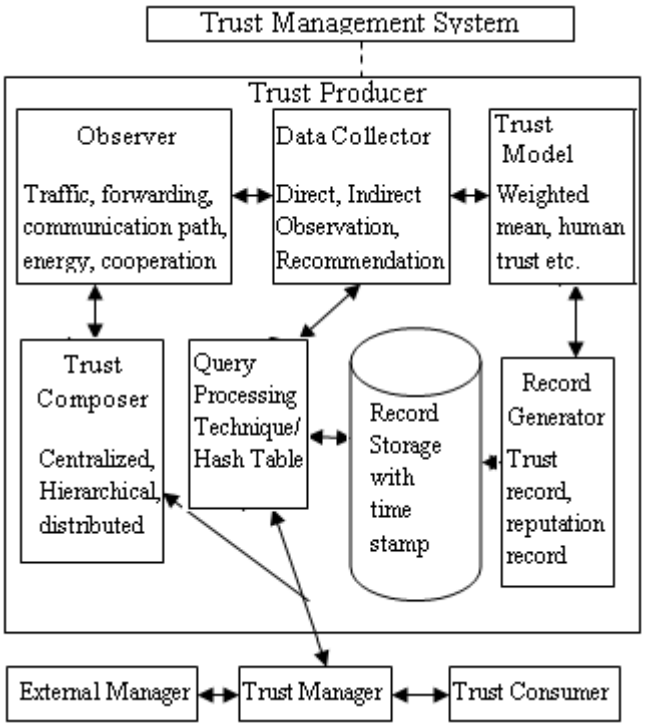

Figure 1: Block Diagram of Trust Management System

Routine cryptography strategies alone are most certainly not satisfactory for secure directing in Wireless Sensor Networks (WSNs). These systems are more defenseless against security assaults because of their assorted applications, absence of supervision and limits in perspective of asset, transforming and stockpiling. To alleviate these issues, trust is generally utilized as an apparatus to give better security by supporting directing conventions. Lately, various specialists have proposed wide assortment of arrangements focused around trust. Nonetheless, all these arrangements convey their own particular configuration. So there is need to design a systematic trust management system [15].

Licensed Under Creative Commons Attribution CC BY

4. Comparison with Other Trusted WSN

Table 1: Comparison of trusted WSN

Scheme	*Trust Metric*	*Direct or Indirect Trust*	*Centralized Distributed or Hybrid scheme*	*Network Architecture supported*
GBTMS [10]	Past interactions	Both	Hybrid	Clustered
HTM [2]	QoS and social trust metrics	Both	Hybrid	Clustered
TCHEM [13]	Data Packets	Both	Distributed	Ad-hoc network
ATRM [14]	Agent based	Both	Hierarchical, Certificate based	Clustered

5. Proposed Idea

The resource efficiency and dependability of a trust system are the most fundamental requirements for any wireless sensor networks (WSN). The clustered wireless sensor networks are incapable of satisfying the resource efficiency and trust system because of the high overhead and low dependability. Light Weight and Dependable Trust System (LDTS) overcomes these limitations using clustering algorithms. LDTS also uses self-adaptive feedback model for trust evaluation. This enhances the energy efficiency and confirms the trustworthiness of nodes that participate in the communication, but there are certain limitations to LDTS as well. The trust values can be analyzed by an intruder and also there is no authentication for the messages being transmitted. In the proposed system, a lightweight simple and robust key generation algorithm is used. This algorithm provides authentication and security for trust messages as well as data messages and results in the design of an energy-efficient, trustworthy and secure communication model in wireless sensor networks.

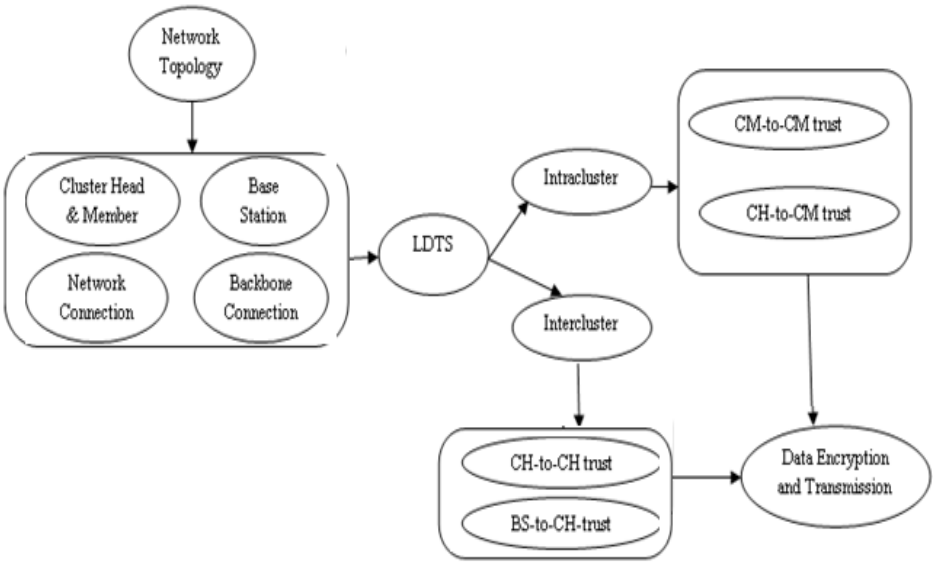

Figure 2: System architecture of trust management System

6. Conclusion

The trust system works on the assumption that a majority of nodes in a neighborhood are dependable. This survey deals with various trusts management schemes for WSNs. Some trust management systems use both direct and indirect observations to calculate the trust value and others use only direct observation to calculate the trust. The trust system is more dependable when both direct and indirect observations are considered. But existing trust systems for wireless sensor network are incapable of satisfying the resource efficiency and dependability of trust system requirements due to high overhead and low dependability. Since Li et al proposed a Lightweight and dependable trust system which demands low memory and communication overhead.

References

[1] G. Theodorakopoulos and J.S. Basras," On trust models and trust evaluation metrics for ad hoc networks," IEEE J. Sel. Areas Commun., vol. 24, no. 2, pp. 318-328, Feb. 2006.

[2] 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 Mang., vol. 9, no. 2, pp. 169-183, Jun. 2012.

[3] 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.

[4] W. B. Heinzelman, A. P. Chandrakasan, and H. Balakrishnan, "An application-specific protocol architecture for wireless microsensor networks," *IEEE Trans. Wireless commun.*, vol. 1, no. 4, pp. 660–670,Oct. 2002.

[5] Z. Liang and W. Shi, "TRECON: A trust-based economic framework for efficient internet routing," IEEE Trans. Syst., Man, Cybern. A, Syst., Humans, vol. 40, no. 1, pp. 52-67, Jan. 2010.

[6] S. Ganeriwal, L. K. Balzano, and M. B. Srivastava,"Reputation-based framework for high

Licensed Under Creative Commons Attribution CC BY

integrity sensor networks," *ACM Trans. Sensor Netw.*, vol. 4, no. 3, pp. 1–37, May 2008.

[7] Y. Sun, W. Yu, Z. Han, and K. J. R. Liu, "Information theoretic framework of trust modeling and evaluation for ad hoc networks," IEEE J. Sel. Areas Commun., vol. 24, no. 2, pp. 305-317, Feb. 2006.

[8] D. Kumar, T. C. Aseri, and R. B. Patel, "EEHC: Energy efficient heterogeneous clustered scheme for wireless sensor networks," *Comput. Commun.*, vol. 32, no. 4, pp. 662–667, Apr. 2009.

[9] O. Younis and S. Fahmy, "HEED: A hybrid, energy-efficient, distributed clustering approach for Ad-Hoc sensor networks," *IEEETrans. Mobile Comput.*, vol. 3, no. 4, pp. 366–379, Oct. 2004.

[10] 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.

[11] S. Zhu, S. Setia, and S. Jajodia, "LEAP: Efficient security mechanisms for large-scale distributed sensor networks," in Proc. 10th ACM Conf. Computer and Comm. Security (CCS'03), 2003, pp. 62-72.

[12] A. Perrig, R. Szewczyk, J. D. Tygar, V. Wen, and D. E. Culler, " SPINS: Security protocols for sensor networks," Wireless. New., vol. 8, no. 5, pp. 521-534, May 2002.

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

[14] A. Boukerche, X. Li, and K. EL-Khatib, "Trust based security for wireless ad hoc and sensor networks," *Computer Commun.*, vol. 30, pp. 2413–2427, Sep. 2007.

[15] P. Raghu Vamsi and Krishna Kant, "Systematic Design of Trust Management Systems for Wireless Sensor Networks: A Review" 2014.

[16] L. Eschenauer, "On Trust Establishment in Mobile Ad-hoc Networks", in *Department of Electrical and Computer Engineering*, vol. Master of Science: University of Maryland, College Park, 2002, pp. 45.

Licensed Under Creative Commons Attribution CC BY