IJISET - International Journal of Innovative Science, Engineering & Technology, Vol. 1 Issue 3, May 2014.
www.ijiset.com
ISSN 2348 - 7968

A Reliable Trust System for Cluster in Wireless Sensor Network

Lavanya Selvaraj[1]
M.Tech II year, Department of IT
V.S.B Engineering College
Karur, Tamil Nadu

Tamizharasan.P[2]
Assistant Professor, Department of IT
V.S.B Engineering College
Karur, Tamil Nadu

***Abstract*— The existing system processes are executed in proposed system also. In addition, the proposed system monitors the sensor nodes produces the actual false positives result nearly similar to the real time environment. A lightweight and dependable trust system (LDTS) proposed for WSNs, employ clustering algorithms. First, a lightweight trust decision-making theme is protected supported on the nodes' identities (roles) within the clustered WSNs, that is appropriate for such WSNs as result of it facilitates energy-saving. Because of canceling feedback between cluster members (CMs) or between cluster heads (CHs), this approach will considerably can improve system potency whereas reduce the result of malicious nodes. More importantly, a lot of significantly CHs war massive amounts of knowledge data forwarding and communication jobs, a dependability-enhanced trust evaluating approach is defined for co operations between CHs. This approach will effectively cut back effectively reduce networking consumption whereas malicious, selfish, and faulty CHs. Moreover, a self-adaptive weighted methodology is outlined for trust aggregation at CH level. Higher than these three square measure primarily wont to solve whereas occurring the attacks(On-off attacks, Sybil Attack and new comer attack and conflicting behavior attack) in between the sender and receiver. In existing to detect and prevent the attacks such as garnished attack and bad mouthing attack. The hash key and lightweight authentication protocol is used for random key generation and to reduce the memory consumption.**

***Index Terms* — a lightweight trust decision-making scheme, A dependability-enhanced trust evaluating approach, A self-adaptive weighted method.**

INTRODUCTION

Wireless sensor networks are composed of inexpensive, small and resource constrained sensor nodes, densely spread over sensing fields that capture diverse types of contextual information related to their environment and make it available to applications and services in other networks and application platforms. The security and the integrity of the data and the communications between sensor nodes are essential requirements for end applications to be reliable. The conventional view of security does not suffice given the unique characteristics of sensor networks that are susceptible to a variety of node misbehaviors. From compromised nodes acting as internal attackers to legitimate nodes that act selfishly, internal misbehaving nodes are a vulnerability that cannot be tackled using authentication and cryptography alone. This vulnerability, along with the cooperative nature of sensor networks, imposes the need for assessing the trust relationships among the network nodes.

The notion of trust, as used in different research areas like trusted computing, trusted platforms, trusted code and trust management, has received various interpretations. Throughout this work, we use the notion of trust as the quantified belief by a trust or with respect to the competence, trust, security and dependability of a trustee within a specified context''. We study the problem of formulating evaluation rules and policies, defining trust evidence, and testing and managing trust relationships, which are collectively referred to as the trust management problem. The main objective of the trust management model proposed in this work is that it should be applied uniformly throughout the sensor network. It should be able to support, through proper configuration, from simple nodes that have very restricted role, computational capabilities and should only trust the nodes they are pre-configured to trust, to highly adaptive nodes and gateways to other networks. The contribution of this paper is a hybrid trust management model that combines aspects from certificate-based and behavior-based approaches on trust establishment on common evaluation metrics in order to allow for flexibility in the trust establishment process, and enables the exploitation of pre-deployment knowledge in order to adjust the supported trust characteristics for each node.

The resource efficiency and dependability of a trust system should undoubtedly be the most fundamental requirements for any WSN (including clustered WSNs). However, existing trust systems created for clustered WSNs are incapable of satisfying these requirements because of their high overhead and low dependability. A universal trust system designed for clustered WSNs for the simultaneous achievement of resource efficiency and dependability remains lacking.

First, limited work has focused on the resource efficiency of clustered WSNs. A trust system should be lightweight to

ISSN 2348 - 7968

serve a large number of resource-constrained nodes in terms of accuracy, convergence speed, and additional overhead [7], [8], [10]. Based on an integrated comparison, a number of innovative works have been developed for clustered WSNs, such as GTMS [13], TCHEM [14], HTMP [15], ATRM [16]. However, most of these works failed to consider the problem of resource constraints of nodes or used complex algorithms to calculate nodes' trustworthiness. Implementing complex trust evaluation algorithms at each CM or CH is unrealistic. Although GTMS uses several novel mechanisms to improve the resource efficiency of clustered WSNs, this approach relies on a broadcast-based strategy to collect feedback among CMs, which requires a significant amount of resource and power.

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 behaviors 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.

b) *Adaptation to risk, leading to flexible security solutions:* The prediction of nodes future behavior 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) *Misbehavior 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.

RELATED WORK

A number of studies have proposed foe WSNs such as [1] this paper describe the Networks together to form hundreds or thousands of cheap micro sensor nodes allows users to accurately monitor and predict the remote environment by efficiently combining the data from the individual nodes. These networks require durable wireless communication protocols that are energy efficient and provide low latency. [12]We develop and analyze low-energy adaptive clustering hierarchy (LEACH), a protocol architecture for micro sensor networks that combines the ideas of energy-efficient cluster-based routing and media access together with application-specific data aggregation to achieve good performance in terms of system lifetime, deferred, and application-perceived quality. LEACH includes a new, administer cluster formation technique that enables self-organization of large numbers of nodes, algorithms for adapting clusters and swapping cluster head positions to evenly distribute the energy load among all the nodes, and techniques to authorize distributed signal processing to save communication resources. Our results display that LEACH can improve system lifetime by an order of magnitude compared with general-purpose multi hop approaches

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 enumuration. 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 behavior, *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

ISSN 2348 - 7968

recommendations. When using beta-function-based methods, the recommendation trust can be calculated as s+1/s+f+1.

c) *Indirect trust:* 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 neighbors 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* – *B*1– *B*2 – … – *Y*, and there may be multiple recommendation paths, such as *A* – *B*1 – *Y*, *A* – *B*2– *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.

LDTS METHOD

It consists of following phases:

A. Network Topology Model

A trust-based framework for cluster-based WSNs as well as a mechanism that reduces the likelihood of compromised or malicious nodes being selected (or elected) as collaborative nodes. A node in the clustered WSN model can be identified as a CH, or a CM.

B. Lightweight Scheme for Trust Decision-Making

LDTS facilitates trust decision-making based on a lightweight scheme. By closely considering the identities of nodes in clustered WSNs, this scheme reduces risk and improves system efficiency while solving the trust evaluation problem when direct evidence is insufficient. A CM calculates the trust value of its neighbors based on two information sources: direct observations (or direct trust degree, DTD) and indirect feedback (or indirect trust degree, ITD). DTD is evaluated by the number of successful and unsuccessful interactions. In this work, interaction refers to the cooperation of two CMs. All CMs communicate via a shared bidirectional wireless channel and operate in the promiscuous mode, that is, if node sends a message to CH via node, then node can hear whether node forwarded such message to CH , the destination.

C. Trust Relationships in LDTS

The trust relationship is generally expressed as a specific quantitative value. This value can be a real number between 0 and 1 or an integer between 0 and 100 (e.g., [8]). In this work, we transform this value into an unsigned integer in the interval between 0 and 10. Although presenting the trust values as a real number or an integer may be insignificant in traditional networks, this issue is of critical importance for WSNs because of limited memory as well as transmission and reception power. This domain of trust values has the following benefits.

D. Less memory overhead

An unsigned integer between 0 and 10 only needs 4 bits (0.5 bytes) of memory space, thus saving save 50%memory space compared with trust values represented as an integer between 0 and 100 (1 bytes) and 87.5% compared with trust values represented as a real number (4 bytes).

E. Less transmission overhead

Given that a smaller number of bits require transmission during the exchange of trust values between nodes, we gain the benefit of less overhead of transmission and reception power.

F. Garnished attack

In such an attack, malicious nodes behave well and badly alternatively with the aim of remaining undetected while causing damage. For instance, garnished malicious nodes may suddenly conduct attacks as they accumulate higher trustworthiness.

G. Bad mouthing attack

As long as feedback is considered, malicious nodes can provide dishonest feedback to frame good parties and/or boost trust values of malicious nodes. This attack, referred to as the bad mouthing attack, is the most effortless attack.

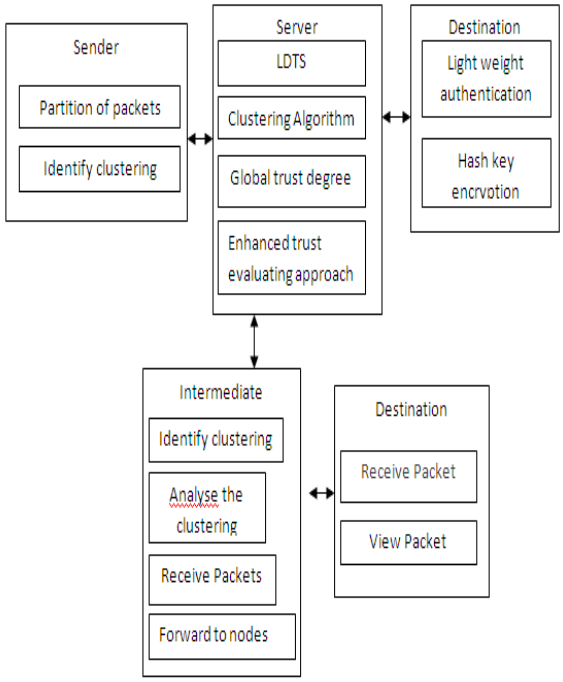

Fig1: System architecture

ISSN 2348 - 7968

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 behavior attacks, Sybil attack and new comer attack ,on off attack and to solve the memory management problem.

REFERENCES

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.

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.

Y. Jin, S. Vural, K. Moessner, and R. Tafazolli, "An energy-efficient clustering solution for wireless sensor networks," *IEEE Trans.Wireless Commun.*, vol. 10, no. 11, pp. 3973–3983, Nov. 2011.

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

[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.

[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, Richard-Wagner-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.

[16] 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

ABOUT THE AUTHORS

Ms.S.Lavanya has received B Tech in Information technology from Anand institute of higher technology and M Tech in Information

ISSN 2348 - 7968

Technology from VSB Engineering College under the Anna University Chennai. Her area of interest includes Mobile computing and network security.

Mr.P.Tamizharasan has received the B.Tech degree from AnnaUniversity and M.Tech degree from Dr M.G.R Educational and Research Institute University. He is currently working as an assistant professor in V S B Engineering College. His area of interest includes Network Security, Data Mining, Stenography, WSN and MANET.