Certain Investigation on Secured Data Transmission in Wireless Sensor Networks

P. Padmaja, S. V. U. College of Engineering, Department of Electrical and Electronic Engineering, Tirupati, India
G.V. Marutheswar, S. V. U. College of Engineering, Department of Electrical and Electronic Engineering, Tirupati, India

ABSTRACT

Wireless Sensor Network (WSN) need to be more secure while transmitting data as well as should be deployed properly to reduce redundancy and energy consumption. WSNs suffer from many constraints, including low computation capability, small memory, limited energy resources, susceptibility to physical capture and the use of insecure wireless communication channels. These constraints make security in WSNs a challenge. In this paper, a survey of security issues in WSNs is presented and a new algorithm TESDA is proposed, which is an optimized energy efficient secured data aggregation technic. The cluster head is rotated based on residual energy after each round of aggregation so that network lifetime increases. Based on deviation factor calculated, the trust weight is assigned, if more deviation, then the trust value is less. Simulation results observed by using NS-2. From network animator and x-graphs the result are analyzed. Among all protocols tesda is an energy efficient secured data aggregation method.

KEYWORDS
BECR, BS, CBQR, CH, CPDA, EESDA, WSN

INTRODUCTION

In WSN, the sensed information of sensor nodes is gathered in different ways such as time driven and event driven. In time-driven approaches, the end user fixes a pre-configured reporting time on each sensor node to collect data from the sensor nodes in a periodic manner. In even driven approaches, the sensor nodes only send the sensing reports to the sink node, when they detect an event.

In WSN, secure data aggregation is crucial to reduce the quantity of data transmission and prolong the lifetime of sensor nodes. The WSN nodes are often compromised, when they are placed in untrusted and hostile environments (Roy et al., 2014). Consequently, the malicious behavior minimizes the security and reliability of the data that are transmitted to the sink node. Hence, trust is an essential factor that specifies the reliability or trustworthiness of sensor node. Considering the trust value of nodes in decision-making process of WSN is crucial, as the WSN collects and combines the sensed data from uncertain environment. Trust is a level of belief of a node that is evaluated based on the node behaviors. In other words, the trust management system allows the nodes to establish a degree of credibility among them based on communication interaction. Consequently, the trust model assists nodes to select a trustworthy adjacent neighbor among its neighbors for data forwarding. Based on
the architecture, trust measurement techniques are categorized into three types such as centralized, distributed, and hybrid.

The centralized trust model comprises a solitary global trusted server that is responsible to determine the trust values of each node in WSN. In distributed trust model, each node locally evaluates the trust values of its one-hop neighboring nodes. Further, the nodes exchange the trust values with other nodes using single or multi hop for making appropriate trust decisions. The hybrid trust model exploits the advantages of both centralized and distributed trust models. The main objective of hybrid trust aware data aggregation model is to minimize the cost that is associated with trust evaluation and enhance the trust accuracy. The hybrid model is utilized with clustering methods in which a CH node acts as a central server to the entire cluster.

LITERATURE SURVEY

The rapid development of data aggregation models increase the security concerns in WSN due to the WSN characteristics of unreliable communication medium and resource constrained nodes. A lot of work has been proposed to ensure security in the data aggregation process (Kumar et al., 2013; Mlaih et al., 2008; Poolsappasit et al., 2012). The conventional security mechanisms are categorized into a credential aware data aggregation and trust-aware data aggregation.

Credential Aware Data Aggregation

The credential aware data aggregation models exploit cryptographic keys, certificates, and hashing functions to attain secure communication in WSN. In key based mechanisms, two nodes that want to establish communication must derive a secure key between them to exchange the data in a secured manner (Winkler et al., 2012). The general idea behind credential aware data aggregation model is to process, relocate, and distribute keys and certificates. Although the credential aware data aggregation models ensure confidentiality and integrity of data, they are vulnerable to snooping and compromised attacks. In addition, the aware credential mechanisms introduce high cost and computational complexity in data aggregation. Therefore, credential aware, secure aggregation methods are not adequate to determine the malicious/selfish nodes and to disparate the corresponding nodes among many benign nodes for secure message routing from sensor nodes to sink. Besides, the resource-limited sensor nodes and necessity of decryption at aggregator node pose significant challenges, when implementing secure data aggregation models in WSN.

Trust-Aware Data Aggregation

In WSNs, the trust-aware data aggregation model plays an important role in detecting the selfish/compromised nodes and also providing high cooperation among trustworthy nodes. The aware trust models enhance the lifetime of networks that stimulate expectations among future interactions. The trust-aware data aggregation model can capture and distribute the trust feedback about recent communication interaction among two sensor nodes. Further, it stores the observed trust information for future routing decisions. Depending on the trust management model, the trust-aware data aggregation models are categorized into centralized, distributed and hybrid model.

In centralized trust management system, a centralized node such as a centralized trusted authority or sink node evaluates the trust value of the nodes in the entire network. The centralized model attains lower overhead, as the high capacity centralized node performs the trust estimation task. Also, the centralized trust model is not appropriate for large-scale WSNs, especially when
Related Content

Packet Dropping Counter Measures in a MANET Through Reliable Routing Protocol Leveraging a Trust Management Framework
www.igi-global.com/article/packet-dropping-counter-measures-in-a-manet-through-reliable-routing-protocol-leveraging-a-trust-management-framework/209390?camid=4v1a

Exploring Personal Mobile Phones and Digital Display Systems to Support Indoor Navigation by Formative Study Methods
www.igi-global.com/article/exploring-personal-mobile-phones-digital/46086?camid=4v1a
Investigating the Roles of Mobile Commerce and Mobile Payment in Global Business
www.igi-global.com/chapter/investigating-the-roles-of-mobile-commerce-and-mobile-payment-in-global-business/183277?camid=4v1a

Perspective and Characteristics of Trust: Understanding Trust in Different Disciplines
www.igi-global.com/chapter/perspective-and-characteristics-of-trust/86915?camid=4v1a