International Journal of Advanced Information Science and Technology (IJAIST) ISSN: 2319:2682
Vol.6, No.10,October 2017 DOI:10.15693/ijaist/2017.v6i10.16-20

SECURE AND TRUSTABLE DATA ROUTING IN WIRELESS SENOR NETWORK: A SURVEY

[1]K.Prema, [2]Dr.N.Thenmozhi

[1]Research scholar, [2]Assistant Professor

[1, 2] Department of computer scienceGovernment Arts college

Coimbatore, India

EMAIL:premakuti@gmail.com, nthenmtu@yahoo.com

***Abstract:*--Wireless sensor network collects the information from insecure environment. The Wireless sensor node has limited power and energy. Sensor network uses a different routing mechanism for collecting the data from sensor nodes. The main challenge while designing the Wireless Sensor Network is to reduce energy utilization and construct effective route strategy to increase lifetime and reliability of the network. For various applications, Wireless Sensor Networks (WSNs) are getting deployed frequently, continuously and they are increasing day by day.In this paper, we review the secure and trustable transmission based routing protocols for securing the data in wireless sensor networks. The normal authentication techniques cannot implement directly in the Wireless sensor network due to less power and energy factors. In the recent research results shows, the security can be improved using modified trusted routing algorithms in the sensor network. This paper collects the trust based secure path routing protocols and analysis based on energy and security properties.**

***Keyterms:*--Wireless sensor networks, Data transmission, Trustable Routing**

I. INTRODUCTION

Wireless Sensor Network is collection or group of specially designed transducers which is having communication infrastructure. It can be used for monitoring, measuring or recording conditions at remote ordiverse locations. Generally measured parameters such as temperature, pressure, speed, humidity, sound intensity, direction of wind, intensity of illumination,voltage of power line, vibration intensity, concentrations of chemicals, pollutants presence level and body functions are used toWSNs have variety of applications like video surveillance, automation of industry, connected smart homes, controlling and monitoring of air traffic and medical equipment, robot control, monitoring atmospheric weather conditions and much more which may be critical to life safety and risk management.

Wireless sensor network connects the distributed wireless sensor nodes in the network. The network should protect the data from inside and outside attackers. Inside attacker attack the network within the network and outside attacker attack from outside the network. The attacker attacks the network either active or passive mode. The active mode alters the network information or data. The passive mode attacks listen the information and do not alter the data or network information. The attacker may have similar capabilities of node to attack the network or have more powerful processors and better battery life.

The network layer control the routing through the intermediate sensor node routing tables. The Wireless sensor nodes have low energy, low computation power, deployed in hostile environments and frequently changing the network topology. So, the normal security protection mechanism cannot be implemented directly. Sensor network has a base station and sensor node. The base stations have more computing power and power compare than sensor node. The sensor node collects the data from the environment and communicate with base stations using different sensor nodes connected in network. The network layer attacks can prevent using link layer encryption and multipath routing. The common security

principle should follow for designing the secured routing.

II. ROUTING IN WIRELESS SENSOR NETWORK

The Routing protocol design is important in wireless sensor network. The data send and receive from the base station and other nodes is based on routing protocols. So, the routingshould be secured using cryptographic mechanism.

A.Routing in wireless sensor network

The sensor nodes communicate with other node using network topology. The routing protocol divided based on network structure and Protocol operation. The network structure routing protocol classified flat based routing, hierarchical based routing and location based routing. The flat-based routing, all the nodes assigned equal roles. The hierarchical based routing, nodes will play different roles in the WSN network. The location based routing, node positions are exploited to route data in the network.

The protocol operation based routing is classified intomultipath-based, query-based, and negotiation-based, QoS-(Quality of Service) based, or coherent-based routing techniques depending on the protocol operation. The data centric routing initiated by sink node. The connected sensor nodes broadcast the message for collecting the data.

The QOS based is routing performed by applying the QOS parameters. The Geographical routing is used location information for routing the data between the nodes. The multipath routingis used multiple path between the sources to destination. This research work focus on the multipath routing which gives more security compare than other routing mechanism in WSN.

B. Attacks on sensor network routing

Many sensor network routing protocols do not consider security when designing the routing protocol. So attacker can easily target to sensor network with routing related attacks.

Selective forwarding attack: It drops the network packets and ensure that the node do not broadcast further in the network. The malicious nodes act as a normal node in the network but it drops or alter the messages. The adversary node may selectively forward the messages. The neighboring node chooses alternative routes. The selectiveforwarding attack is hard to detect.

Altering routing Information: Thisattack alter the routing information exchanged between the sensor nodes. The adversaries nodeisable to create routing loops, generate alternative routing paths and generate fault error messages.

Byzantine attack: It compromises the sensor node and programmed to transmit the messages. It confuses the routing decision maker and randomly disrupts the system. It can be Flood Rushing Attack and Black Hole Attack. Black Hole Attack drops the network messages but participate in all wireless sensor network communication. Flood RushingAttack gives preference to affected message instead of genuine message.

Sinkhole attack: This attacks are difficult to defend and it is used to advertise information such as more energy or more reliability to construct the route.Some protocols verify the quality of the routing information. When the malicious node added in the wireless sensor network, it controls the messages passed between the sensor nodes.

Compromised node: The sensor node deployed in a hostile environment and it is not able to monitor the network topology. The sensor node compromise by the attacker and the attacker get all the required information about the network or sensor node. If the sensor node has any cryptographic information, the attacker can fmd the keys and intrude the network.

Denial of service (DOS): This attack tries to send unnecessary packets and utilize more network

bandwidth. It prevents the network user from accessing the service or resource which they need to communicate. The DoSattack could be in Physical layer, link layer, network layer and transport layer. The DoS attack can be prevented by strong authentication and identification and use Instruction detection system.

Wormhole attack: The wormhole attack records the messages in wireless sensor network and channels to another location. The tunneling process can wormhole the attack and can retransmit messages selectively. This attack relatively coupled with selective forwarding and Sybil attack and difficult to detect.

Sybil attack: The malicious sensor node illegally claims multiple identities. The attacker can generate

many sensor node identification using a single physical device. The WSN use gateway for preventing Sybil type attacks.

III. SECURE AND TRUSTABLE ROUTING IN WSN

Many organizations have the opinion that security and privacy are to protect our data. The difference is that the security is implemented to ensure privacy. In other words, security is the sealed envelope and privacy isthe successful delivery of the message inside the envelope. This survey besides pioneer in classifying secured routing protocols that reveals securitygains, security losses and security loopholes based on the technique used by the algorithms.

A. Target Detection with Sensing Frequency

Target Detection with Sensing Frequency K(TDSFK) scheme is proposed by Yanling Hu, et al [1]. The important issue is the balance between the quality of target detection and lifetime in wireless sensor networks. Two target-monitoring schemes are proposed. One of the scheme is Target Detection with Sensing Frequency K(TDSFK), which distributes the sensing time that currently is only on a portion of the sensing period into the entire sensing period. That is, the sensing frequency increases from 1 to K. The other scheme is Target Detection with Adjustable Sensing Frequency (TDASF), which adjusts the sensing frequency on those nodes that have residual energy. The simulation results showed that the TDASF scheme can improve the network lifetime by more than 17.4% and can reduce the weighted detection delay by more than 101.6%

B. Broadcasting Combined with Multi-NACK/ACK

Broadcasting Combined with Multi-NACK/ACK (BCMN/A) protocol is proposed by Mianxiong Dong,et.al[2]. A data gathering protocol is proposed based on the analysis strategy. Proposedprotocol achieves energy and delay efficiency during the data

gathering process both in intra-cluster and inter-cluster. In intra-cluster, after each round of TDMA collection, a cluster head broadcasts NACK to indicate nodes which fail to send data in order to prevent nodes that successfully send data from retransmission. This work first presented an analysis sensing application through trade-offs between the energy consumption (lifetime) and source-to-sink transport delay under reliability constraint wireless sensor networks.

C. Energy Provisioning in Rechargeable Networks

Wireless identification and sensing platform (WISP) and commercial off-the-shelf RFID readers techniques is proposed by Shibo et al[3].WISP tags served as sensors and can harvest energy from RF signals transmitted by the readers. This kind of WRSNs is highly desirable for indoor sensing and activity recognition and is gaining attention in the research community. One fundamental question in WRSN design is how to deploy readers in a network to ensure that the WISP tags can harvest sufficient energy for continuous operation and based on a practical wireless recharge model supported by experimental data, it investigated two forms of the problem such as point provisioning and path provisioning. Point provisioning is used the least number of readers to ensure that a static tag placed in any position of the network that will receive a sufficient recharge rate for sustained operation. Path provisioning exploits the potential mobility of tags to further reduce the number of readers necessary: mobile tags can harvest excess energy in power-rich regions and store it for later use in power-deficient regions.

D. Service Pricing Decision in Cyber-Physical Systems

A game based services price decision (GSPD) model is proposed by Xiao Liu, et al [4]. Cyber-Physical Systems (CPS), Service Organizers (SOs) aimed to collect service from service entities at lower price and providedbetter combined services to the users. Itformulated the price competition model of SOs where the SOs dynamically increase and decrease their service prices periodically according to the number of collected services from entities. A game based services price

decision (GSPD) model which depicts the process of price decisions is proposed. In the GSPD model, entities game with other entities under the rule of "survival of the fittest" and calculate payoffs according to their own payoff-matrix, which leads to a Pareto-optimal equilibrium point.

E. Authenticated Trust and Reputation Calculation and Management System

A novel authenticated trust and reputation calculation and management (ATRCM)technique is proposed by ChunshengZhu,etal[5]. This authorincorporate the powerful data storage and data processing abilities of cloud computing (CC) as well as ubiquitous data gathering capability of wireless sensor networks (WSNs), CC-WSN integration received a lot of

attention from both academia and industry.In this work proposed a novel authenticated trust and reputation calculation and management (ATRCM) system for CC-WSN integration. Considering the authenticity of CSP and SNP, the attribute requirement of cloud service user (CSU) and CSP, the cost, trust, and reputation of the service of CSP and SNP, the proposed ATRCM system achieves the following three functions: 1) authenticating CSP and SNP to avoid malicious impersonation attacks; 2) calculating and managing trust and reputation regarding the service of CSP and SNP; and 3) helping CSU choose desirable CSP and assisting CSP in selecting appropriate SNP.

F. PHACK -Selective Forwarding Attack Detection

Per-Hop Acknowledgement (PHACK)-based scheme is proposed by Anfeng Liu, et al[6]. Each packet transmission is to detect selective forwarding attacks. In this scheme, the sink and each node along the forwarding path generate an acknowledgement (ACK) message for each received packet to confirm the normal packet transmission.

The scheme, in which each ACK is returned to the source node along a different routing path, can significantly increase the resilience against attacks because it prevents an attacker from compromising nodes in the return routing path, which can otherwise interrupt the return of nodes ACK packets.Inthis case, the PHACK scheme also has better potential to detect abnormal packet loss and identify suspect nodes as well as better resilience against attacks. Another pivotal issue is the network lifetime of the PHACK scheme, as it generates more acknowledgements than previous ACK-based schemes.

G. Deployment guidelines for achieving maximum lifetime

Deployment guidelines for achieving maximum lifetime approach is proposed by AnfengLiua,et at [7]. It is characterized the energy consumption of wireless sensor networks with adjustable transmission ranges through theoretical analysis. Based on this result, it should a deployment strategy with T as the required minimum network lifetime.

There are three interventions: (A) in order to achieve an evenly balanced energy consumption among all nodes, the node density in different areas of the network should be a continuous varying function of the distance from the sink; (B) if there are insufficient nodes to achieve a balanced energy consumption over the whole network, it proposed node deployment strategy can be used to achieve the required lifetime threshold T with minimum number of nodes; and (C) when there are sufficient nodes to ensure the network connectivity and coverage with the node density of s, designed an algorithm to identify the optimal transmission radius rand the corresponding achievable maximum network lifetime.

V. CONCLUSION

This work surveyed various secured routing models and techniques used to improve the security and network efficiency by multipath routing in WSN. Since the security is the core concept of data transmission and various mechanisms in networking environment. The routing mechanism changes according to the evolution methods at different levels of networks. Finally, the potential benefits of applying secure and trustabledata routing in combination with a general security model in this area are highlighted.This combination can give a significant impact, especially regarding the strong authentication and attacker detection of general routing and data sharingsolutions.Future work of this researchwill involve the evaluation of these possibilities.

REFERENCES

[1]. Y. Hu, M. Dong, K. Ota, et al. "Mobile Target Detection in Wireless Sensor Networks with Adjustable Sensing Frequency," IEEE System Journal, Doi: 10.1109/JSYST.2014.2308391, 2014.

[2]. M. Dong, K. Ota, A. Liu, et al. "Joint Optimization of Lifetime and Transport Delay under Reliability Constraint Wireless Sensor Networks," IEEE Transactions on Parallel and Distributed Systems, vol. 27, no. 1, 2016.

[3]. S. He, J. Chen, F. Jiang, et al. "Energy provisioning in wireless rechargeable sensor networks," IEEE transactions on mobile computing, vol. 12, no. 10, pp. 1931-1942, 2013.

[4]. X. Liu, M. Dong, K. Ota, P. Hung, A. Liu. "Service Pricing Decision in Cyber-Physical Systems: Insights from Game Theory," IEEE Transactions on Services Computing, vol. 9, no. 2, pp. 186-198, 2016.

[5]. C. Zhu, H. Nicanfar, V. C. M. Leung, et al. "An Authenticated Trust and Reputation Calculation and Management System for Cloud and Sensor Networks Integration," IEEE Transactions on Information Forensics and Security, vol. 10, no. 1, pp. 118-131, 2015.

[6]. Liu, M. Dong, K. Ota, et al. "PHACK：An Efficient Scheme for Selective Forwarding Attack Detecting in WSNs," Sensors, vol. 15, no. 12, pp. 30942-30963, 2015.

[7]. Liu, X. Jin, G. Cui, Z. Chen, "Deployment guidelines for achieving maximum lifetime and avoiding energy holes in sensor network,"Information Sciences, vol. 230, 2013.

[8]. Z. Zheng, A. Liu, L. Cai, et al. "Energy and Memory Efficient Clone Detection in Wireless Sensor Networks," IEEE Transactions on Mobile Computing.vol. 15, no. 5, pp. 1130-1143, 2016.

[9]. T. Shu, M. Krunz, S. Liu, "Secure data collection in wireless sensor networks using randomized dispersive routes," IEEE Transactions on Mobile Computing, vol. 9, no. 7, 2010.

[10]. P. Zhou, S. Jiang, A. Irissappane, et al. "Toward Energy-Efficient Trust System Through Watchdog Optimization for WSNs," IEEE Transactions on Information Forensics and Security, vol. 10, no. 3, pp. 613-625, 2015.

[11]. S. Shen, H. Li, R. Han, et al. "Differential game-based strategies for preventing malware propagation in wireless sensor networks," IEEE Transactions on Information Forensics and Security, vol.9, no. 11, pp. 1962-1973, 2014.

[12]. O. Souihli, M. Frikha, B. H. Mahmoud, "Load-balancing in MANET shortest-path routing protocols," Ad Hoc Networks, vol.7, no.2, 2009.
[13]. J. Long, A. Liu, M. Dong, et al. "An energy-efficient and sink-location privacy enhanced scheme for WSNs through ring based routing," Journal of Parallel and Distributed Computing, vol. 81, pp. 47-65, 2015.
[14]. S. He, J. Chen, X. Li, et al. "Mobility and intruder prior information improving the barrier coverage of sparse sensor networks," IEEE transactions on mobile computing, vol. 13, no. 6, pp.1268-1282, 2015.
[15]. S. H. Seo, J. Won, S. Sultana, et al. "Effective key management in dynamic wireless sensor networks," IEEE Transactions on Information Forensics and Security, vol. 10, no. 2, pp. 371-383, 2014.
[16]. Y. Hu, A. Liu. "An efficient heuristic subtraction deployment strategy to guarantee quality of event detection for WSNs," The Computer Journal, vol. 58, no. 8, pp. 2015.
[17]. S. J. Lee, M. Gerla, "Split Multipath Routing with Maximally Disjoint Paths in Ad Hoc Networks," IEEE ICC, pp. 3201-3205, 2011.
[18]. Y. Zhang, S. He, J. Chen. "Data Gathering Optimization by Dynamic Sensing and Routing in Rechargeable Sensor Networks," IEEE/ACM Transactions on network, doi:10.1109/TNET.2015.2425146, 2015.
[19]. P. Nghiem, T. H. Cho, "A multi-path interleaved hop-by-hop en-route filtering scheme in wireless sensor networks," Computer Communications, vol. 33, no. 10, pp. 1202-1209, 2010.
[20]. Y. L. Yu, K. Q. Li, W. L. Zhou, P. Li, "Trust mechanisms in wireless sensor networks: Attack analysis and countermeasures," Journal of Network and Computer Applications, vol. 35, no. 3,pp. 867-880, 2012.

AUTHOR PROFILE

K.Prema received the UG degree in Bsc computer science from Pioneer college of Arts and science 2014, then received the PG degree in Master of Computer science from KG college of Arts and science 2016 currently doing MPhil in computer science from Gov Arts college Coimbatore.