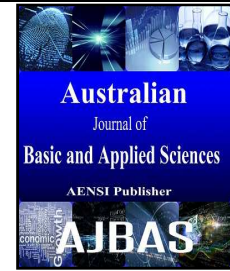




AUSTRALIAN JOURNAL OF BASIC AND APPLIED SCIENCES

ISSN:1991-8178 EISSN: 2309-8414
Journal home page: www.ajbasweb.com



Symmetric Key Encryption for Secure Communication Using Wireless Hart In Wireless Sensor Networks (WSN)

¹P. Pritto Paul, ²Dr.N.Sankar Ram and ³M. Usha

¹Research Scholar Department of CSE Velammal Engineering College Chennai, India

²Professor and Head, Department of CSE, RMK College of Engg and Tech Chennai, India

³Assistant Professor, Department of CSE, Velammal Engineering College Chennai, India

Address For Correspondence:

P. Pritto Paul, Research Scholar Department of CSE Velammal Engineering College Chennai, India
E-mail: p.prittopaul@gmail.com

ARTICLE INFO

Article history:

Received 12 February 2016

Accepted 12 March 2016

Available online 20 March 2016

Keywords:

Hierarchical Clustering,
WirelessHART, ClusterHead (CH),
WirelessHART Communication
Protocol, WSN, Protocols.

ABSTRACT

Security is the most questing issue in Wireless Sensor Network (WSN) now-a-days because of various attacks on mobile nodes. Since existing security mechanisms are inadequate, new ideas are needed to effectively address the wireless sensor network security. Since a low energy node is more prone to security attacks, secure routing algorithms that consume less energy for communication should be used. Most of the real-world wireless sensor networking applications requires a certain amount of trust in their application in order to maintain proper network functionality. WirelessHART is an emerging secure and reliable communication standard that aims in maximizing the utilization of wireless communication. This paper employs the WirelessHART communication protocol for secure communication between two nodes. The WirelessHART standard is implemented on individual sensor nodes to ensure security. To reduce the communication overhead, hierarchical clustering is performed and sensor nodes are allowed to communicate only based on their trust value.

INTRODUCTION

Wireless Sensor Networks (WSNs) consist of multiple sensor nodes with sensing, computation, and wireless communications capabilities. The main aim of Wireless Sensor Network (WSN) is to collect data from the environment (Du, X., H.H. Chen, 2008). Wireless Sensor Network (WSN) is employed in harsh environments where pure human access and monitoring cannot be easily scheduled or efficiently managed. Wireless sensor networks are employed mostly in public and uncontrolled areas; hence the security is a major challenge (Giruka, V.C., 2008). The traditional security mechanisms are authentication, symmetric key and Public Key Infrastructure (PKI) cryptography. WSN includes many different types of sensors such as seismic, low sampling rate magnetic, thermal, visual, infrared, acoustic and radar, which are able to monitor a wide variety of ambient conditions (Raman, S., 2010). WSN finds its applications in military, environment, health, home and other commercial areas. WirelessHART is a secure and reliable communication standard employed widely for industrial process automation. WirelessHART uses 2.4GHz frequency band, a free unlicensed portion of the spectrum. Channel Hopping can be used to avoid interference among frequency bands which enhances reliability. WirelessHART is a self-healing and self-organizing protocol which can find its neighbours and establish path with those neighbours by channel hopping and synchronization information and measuring signal strength. WirelessHART network includes wired entities such as Network Manager, Gateway, Security Manager, Plant Automation Hosts (PAH) and wireless entities such as Field Devices, Adapters, Routers, Access Points and Handheld Devices (Umarani, V., K.S. Sundaram, 2013). Security in WirelessHART standard can be divided into three levels such as End-to-End, Per-hop and Peer-to-Peer. Security in WirelessHART is enforced

Open Access Journal

Published BY AENSI Publication

© 2016 AENSI Publisher All rights reserved

This work is licensed under the Creative Commons Attribution International License (CC BY).

<http://creativecommons.org/licenses/by/4.0/>



Open Access

To Cite This Article: P. Pritto Paul, Dr.N.Sankar Ram and M. Usha., Symmetric Key Encryption for Secure Communication Using Wireless Hart In Wireless Sensor Networks (WSN). *Aust. J. Basic & Appl. Sci.*, 10(1): 625-630, 2016

in Network Layer and Data Link Layer. Data Link Layer provides hop-to-hop security between two devices using Network key; and Network Layer enforces end-to-end security between source and destination using session key(s) and/or join key. Network Layer in WirelessHART protocol stack provides Confidentiality, Integrity and Authentication. Advanced Encryption Standard (AES-128 bit) can be used to achieve security in a WirelessHART network. To identify the malicious nodes in a network, a trust model is required. A trust model supports decision making in a Wireless Sensor Network (WSN) such as pre key-distribution, data aggregation, sink node selection and self-reconfiguration of these sensor nodes. Trust model encourages trustworthy nodes to communicate but it discourages untrustworthy nodes to even participate in the network (Boukerch, A., 2007). Trust also increases network lifetime, throughput and resilience in a WSN. Trust may be subjective or objective depending on the task. In general, trust is classified as behavioral or computational trust based on where it is used. Behavioral trust defines trust relations among people and organizations. Computational trust defines trust relation among devices, computers, and networks. Depending on the observation, trust may be direct trust or indirect trust. Direct trust specifies the direct observations and called as first hand information. Indirect trust specifies the indirect observation and called as second hand information.

II. Trusted routing in wireless sensor networks (wsn):

Various routing, power management, and data dissemination protocols have been specifically designed for WSNs where energy consumption is an essential design issue.

2.1. Classification of Routing Protocols:

Since WSN protocols are application-specific, the focus is given to the routing protocols that differ depending on the application and network architecture. The three main categories of routing protocols are data-centric, hierarchical and location-based. Fig. 3 shows the classification of the routing protocols.

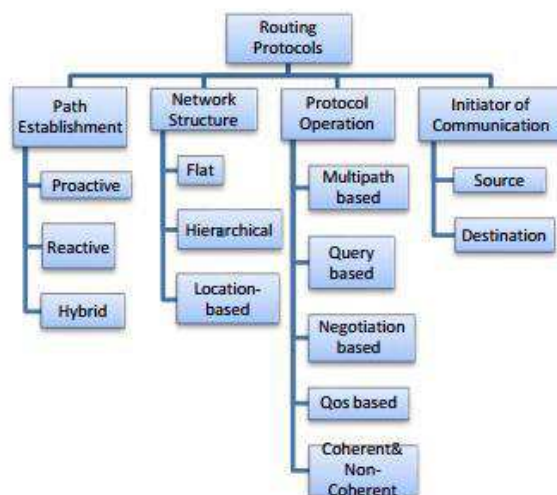


Fig. 1: Classification of Routing Protocols in WSN.

2.2. Structure of Trust Model:

In a network, trust helps a node to determine whether its neighbour node is uncooperative or malicious. In an Ad-hoc network, trust plays a major role in detecting misbehaviours, routing and resource sharing. The advantages and disadvantages of a trust model are given in Table II.

Table 1: The Structure of a Trust Model- Pros and Cons.

Structure	Pros	Cons
Centralized	Less computation	Communication overhead, less reliable and no scalability
Distributed	Reliable and scalable	Computation overhead
Hybrid	Less communication overhead than centralized	Large computation overhead and memory requirements than centralized; less reliable and scalable than distributed

2.3. Various Trust Models:

In WSN, trust plays a major role in detecting a malicious node. The reputation-based framework for high integrity sensor network (RFSN) (Alzaid, H., 2008) utilizes the watchdog mechanism to collect data and monitor different events in the node to build reputation thereby getting the trust rating of that node. The LDTS is a lightweight trust system for clustered wireless sensor networks which uses direct trust and feedback trust to enhance decision making and collaborative processing by detecting malicious behaviour. The hierarchical trust management for wireless sensor networks (HTMW) performs multi-path routing to evaluate trustworthiness of a node using subjective trust and objective trust. The bio-inspired trust and reputation model (BTRM-WSN) (Xiang, G., 2012) uses the distributed based ant colony approach to improve the collaboration among nodes by selecting most trustworthy nodes along the path from a sensor node to its sink node. The agent based trust management (ATRM) (Zhang, J., 2010) approach employs distributed certificate based trust model to monitor the behaviour of network with the help of agent module. The TMA (Ganeriwal, S., 2008) is dynamic certification based trust management architecture for hierarchical WSN that lowers the computation and communication overhead by considering both behavioural and direct trust. The reliable data aggregation and transmission protocol (RDAT) (Chen, D., 2011) is a distributed function based beta reputation model which amends the reliability of data aggregation and transmission by evaluating each sensor node's action using a respective function reputation. The reputation-based secure data aggregation (RSDA) improves the accuracy of aggregated data and enhance the network lifetime. The trust management model for internet of things (TRM-IoT) (Ozdemir, S., 2008) is a fuzzy based reputation model which provides efficient and safe communication from source to destination. The addition encouragement and multiplication punishment (AEMP) (Mármol, F.G., G.M. Pérez, 2011) is a new routing trust based protocol that enhances WSN ability against attacks from within the network. The direct trust dependent link state routing protocol (DTLSRP) (Kahn, J.M., 1999) is a trust based routing protocol that protects network from routing attacks. The distributed reputation based beacon trust system (DRBTS) (Babu, S.S., 2011) is a reputation based distributed structure which helps to monitor misbehaviours in WSN. The TMA is dynamic certification based trust management architecture for hierarchical WSN that considers behavioural and direct trust and reduces the computation and communication overhead. TABLE III shows various techniques that can be used to build a trust model in sensor networks.

III. Wireless hart communication protocol:

Figure 2 represents a generic WirelessHART network architecture. It is formed by a group of network devices that can either be a field device which is directly connected to the process plant, or handheld devices. The network supports two topologies: direct connection between device and gateway (star topology) and connections over multiple hops (mesh topology). Each network device must therefore be able to act as source, sink and router. The WirelessHART gateway serves as a bridge connecting the WirelessHART network to the process plant. It includes a virtual gateway and one or more network access points. Host applications can access the network devices through the service interface, which can have single or multiple ports.

Operators are also allowed to monitor or configure particular field device through the process plant backbone. These network access points provide the actual physical connection to the WirelessHART network. The virtual gateway serves as the sink and source for the network traffic. It should be a HART type device, namely one that supports all HART application commands and also able to translate cached data that can be interpreted by the host applications. The gateway also provides buffering for burst and large data transfers, command responses, event notification and diagnostics. The virtual gateway communicates directly with the network manager, which configures and maintains the WirelessHART network. Each network consists of only one network manager. The manager requests information from field devices via the gateway to make certain decisions. The host application can also provide input to the network manager. The security manager works along with the network manager to prevent possible intrusions and attacks to the WirelessHART network. Multiple networks can be connected to one security manager. It generates session keys, joint keys and network key. These keys are further propagated to the field devices by the network manager. The WirelessHART standard specifies the communication protocol stack using the OSI model. At the bottom is the physical layer which is responsible for signalling, modulation and actual transmission of data. Above that is the data link layer which determines how common wireless medium is shared between the network devices. It is also responsible for formatting data packets, detection/correction of bit errors. The network layer is the core of the WirelessHART standard which is responsible for routing, topology control, end-to-end security and session management. The transport layer ensures end-to-end transmission reliability and flow control.

3.1. Network Manager:

The network manager maintains the health of a WirelessHART network. When a WirelessHART network gets initialized, a unique network ID along with security keys from the security manager will be provided to the network manager. It establishes the connection with the gateway and the network access points to secure the bandwidth needed for management and control packets going to and from the network devices. When a new

device wants to join the network, the manager validates its integrity using join keys and the network ID to ensure its trustworthiness and whether it is joining the right network. Once authenticated, the network manager provides the device with necessary network and session keys from the security manager and assigns a 16 bit network address. It is required that a device has at least two neighbours to ensure path diversity and hence better reliability.

Table 2: Trust Models in WSN.

Trust Model	Purpose	Structure	Trust
			Computational
RFSN [9]	To monitor fraudulence in the network	Distributed and cooperative	Beta distribution approach
ATRM [10]	To minimize overhead	Hierarchical Certificate based	Agent based
DRBTS [11]	To monitor fraudulence in the network	Distributed and cooperative	Quorum voting approach
AEMP [12]	To support secure routing	Distributed	Weighted approach
RDAT [13]	To improve the reliability of data aggregation	Distributed	Beta distribution
TRM-IoT [14]	To build collaboration among nodes	Distributed and Behavior based	Fuzzy
BTRM [15]	To pick out trustworthy Nodes	Distributed	Ant colony
DTLSRP [16]	To discover trust based routing	Distributed	Weight
TMA [17]	To minimize communication and storage overhead	Behavior and Certificate based Hierarchical	Weight based
RSDA [18]	To amend accuracy of aggregated data	Distributed	Beta probability Density
LDTS [19]	To help collaborative processing by detecting malicious behaviour	Hierarchical	Weight based Approach
HTMW [20]	To execute routing and intrusion detection	Hierarchical	Stochastic Petri net

3.2. Transport Layer:

Block data transfer mechanism is the unique feature of the WirelessHART transport layer. It establishes a connection oriented communication link between the host application and the field device. The host application configures the slave device by opening a port onboard the device using a HART command. The port specifications are also part of the WirelessHART standard. Once the port is opened, transmission rate between the device and host application is negotiated with the network manager to maximize the throughput. Block data transfer should be reliable and end-to-end acknowledgement is required to keep track of the data stream. This

may require the network manager to update its routing and scheduling plan to provide the necessary priority.

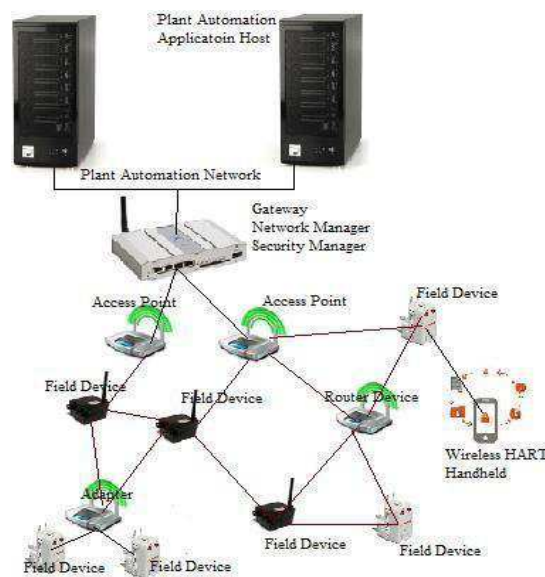


Fig. 2: Wireless HART Network Architecture.

RESULTS AND DISCUSSIONS

In this paper, we are comparing two routing protocols namely, the Ad-Hoc On Demand Distance Vector (AODV) routing protocol which is used for mobile data transmission and our new routing protocol, which is the WirelessHART Communication Protocol (WHCP). We simulated the comparison using NS2 and obtained the result as follows from our trace map.

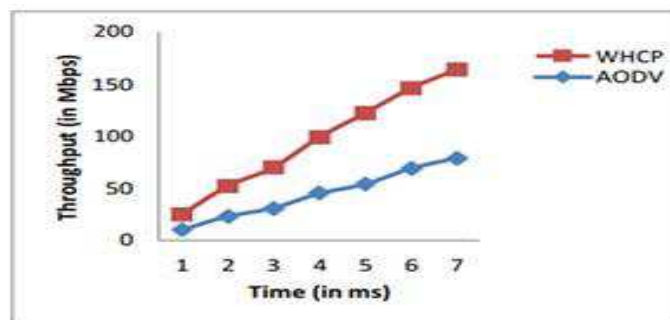


Fig.3 Performance Evaluation of AODV and WHCP

Figure 3 shows the comparison graph of AODV and WHCP routing protocols in terms of their throughput. Here we observe that, after the completion of the tenth round, AODV protocol takes more time to transmit the data to the base station (BS) than WHCP. The major reason behind this is that in case of AODV protocol, the route discovery cycle takes more time. Hence, it is clear that WHCP routing protocol is more secure and effective than AODV routing protocol.

V. Conclusion and future work:

This paper is the first one to apply the ideas of WirelessHART standard to provide security in a hierarchical clustered network. We have paid special attention to issues that are important to achieve a stable and secure data transmission. The trust and trust relationship among nodes further enhances the security. Based on these trust relationships, they can also perform trusted routing. The communication overheads are also greatly reduced since we have applied hierarchical clustering to the entire network. Upgrades can also be incorporated into WirelessHART to improve the network performance. Even with the existing gateways, the network lifetime can be improved by routing data to different virtual gateways/access points. Mobile gateways can be used to balance the load distribution in the network. In the future, we will optimize our WirelessHART Communication Protocol and establish some fast response mechanisms when malicious behaviours of attackers are detected. We will also

work on applying this WirelessHART protocol into various applications and other routing protocols of Wireless Sensor Networks (WSN). We will conduct a detailed simulation in terms of message overhead, security analysis, and tolerance to intruders.

REFERENCES

- Du, X., H.H. Chen, 2008. Security in wireless sensor networks. *Wireless Communications, IEEE*, 15(4): 60-66.
- Abbasi, A.A., M. Younis, 2007. A survey on clustering algorithms for wireless sensor networks. *Computer communications*, 30(14): 2826-2841.
- Giruka, V.C., M. Singhal, J. Royalty, S.V. aranasi, 2008. Security in wireless sensor networks. *Wireless communications and mobile computing*, 8(1): 1-24.
- Raman, S., A. Prakash, K.B. Pulla, P. Srivastava, A. Srivastava, S. Singh, 2010. Wireless sensor networks: A Survey of Intrusions and their Explored Remedies. *International Journal of Engineering Science and Technology*, 2(5): 962-969.
- Umarani, V., K.S. Sundaram, 2013. Survey of Various Trust Models and Their Behavior in Wireless Sensor Networks.
- Boukerch, A., L. Xu, K. El-Khatib, 2007. Trust-based security for wireless ad hoc and sensor networks. *Computer Communications*, 30(11): 2413-2427.
- Bao, F., I.R. Chen, M. Chang, J.H. Cho, 2012. Hierarchical trust management for wireless sensor networks and its applications to trust-based routing and intrusion detection. *Network and Service Management, IEEE Transactions on*, 9(2): 169-183.
- Li, X., F. Zhou, J. Du, 2013. LDTS: a lightweight and dependable trust system for clustered wireless sensor networks. *Information Forensics and Security, IEEE Transactions on*, 8(6): 924-935.
- Alzaid, H., E. Foo, J.G. Nieto, 2008. RSDA: reputation-based secure data aggregation in wireless sensor networks. In *Parallel and Distributed Computing, Applications and Technologies, PDCAT. Ninth International Conference on* (pp: 419-424). IEEE.
- Zhang, J., R. Shankaran, M.A. Orgun, V. Varadharajan, A. Sattar, 2010. A trust management architecture for hierarchical wireless sensor networks. In *Local Computer Networks (LCN), 2010 IEEE 35th Conference on* (pp: 264-267). IEEE.
- Babu, S.S., A. Raha, M.K. Naskar, 2011. A Direct trust dependent link state routing protocol using route trusts for WSNs (DTLSRP). *Wireless Sensor Network*, 3(04): 125.
- Mármol, F.G., G.M. Pérez, 2011. Providing trust in wireless sensor networks using a bio-inspired technique. *Telecommunication systems*, 46(2): 163-180.
- Chen, D., G. Chang, D. Sun, J. Li, J. Jia, X. Wang, 2011. TRM-IoT: a trust management model based on fuzzy reputation for internet of things. *Computer Science and Information Systems*, 8(4): 1207-1228.
- Ozdemir, S., 2008. Functional reputation based reliable data aggregation and transmission for wireless sensor networks. *Computer Communications*, 31(17): 3941-3953.
- Xiang, G., Q. Jianlin, W. Jin, 2012. Research on trust model of sensor nodes in WSNs. *Procedia Engineering*, 29: 909-913.
- Kahn, J.M., R.H. Katz, K.S. Pister, 1999. Next century challenges: mobile networking for "Smart Dust". In *Proceedings of the 5th annual ACM/IEEE international conference on Mobile computing and networking* (pp: 271-278). ACM.
- Ganeriwal, S., L.K. Balzano, M.B. Srivastava, 2008. Reputation-based framework for high integrity sensor networks. *ACM Transactions on Sensor Networks (TOSN)*, 4(3): 15.