Secure Multipath routing Protocols in Wireless Sensor Network: a survey Analysis

Dr. A. Senthilkumar
Professor, Department of MCA
Sengunthar Engineering College, Tamilnadu, India
senthilkumarmca76@gmail.com

***Abstract*— Wireless sensor network (WSN) connects the distributed autonomous sensors for collecting the data from sensors or distribute the data into sensors. The WSN uses in military applications, machine and environmental health monitoring, home monitoring, Air pollution monitoring, fire detection and more industries. The attacker use Compromised node, Node capture attacks, Denial of service (DOS), Altering routing Information, Selective forwarding attack, sinkhole attack, wormhole attack, Sybil attack, Byzantine attack and more network attacks in Wireless sensor networks. Due to limited resources in wireless sensor network, the security will be bigger concern in wireless sensor networks. Wireless sensor network routing protocols do not give much importance to security and give importance to performance and power source factors while design the routing protocols. This paper analysis the recent survey in secure multipath routing protocols in wireless sensor network based on information security principals and attack types. It helps researchers to understand the recent secure multipath protocols.**

***Keywords*— Multipath routing; WSN; security; survey;**

I. INTRODUCTION

The sensor is a node in the wireless sensor network which has microcontroller, transceiver, external memory, power source, Transceiver and one or more sensors. The wireless sensor network connects the distributed autonomous sensors. WSN uses in military applications, Earthquake Early Warning Systems, machine and environmental health monitoring, home monitoring, Air pollution monitoring, fire detection and more industries. The sensor node is a small component which cannot compute more computation process due to less resource power. The sensor node connected using wireless network. The wireless sensor network classified in two types (1) Data Acquisition Network (2) Data Distribution Network. The Data Acquisition Network collects the data from autonomous sensor nodes and Data Distribution Network distribute the data into sensor nodes connected to the network.

The wireless sensor node has limited Power supply, low Bandwidth between sensor networks and low computational power. So, the traditional network future cannot apply directly in Wireless sensor network. In a wireless sensor network, the data send or receive between the sensor nodes, sensor to the base station and base station to the sensor, base station to management center. The base station is a node which has more computational power and bandwidth compare than the sensor nodes.

II. SECURITY IN WSN

The security in Information technology classified into five types. (1) Application security (2) Computing security (3) Data security (4) Information security and (5) Network security. The application security measures through the Software Development Lifecycle (SDLC). The Computer security help to prevent unauthorized access to the computer. Network security prevents unauthorized access to the computer network which controlled by the network administrator.

The information security gives the five security principal (1) Confidentiality (2) Authenticity (3) Integrity and (4) Availability and (5) Data Freshness [18]. [14] gives the explanation for each security principal. The Confidentiality prevents unauthorized access from an attacker. The attacker will not understand the message. The Authenticity makes sure reliability between the communication entities. The Integrity provides the mechanism for knowing whether the message tampered or not. It makes sure the message can be accessed only authorized parties. The Availability make sure the system or service should available and should not affected by any attacks. Data Freshness makes sure the fresh data communication between the communication entities. Most of the multipath routing protocols in WSN may not consider the above security principal while design the protocol [18]. The secured protocol cost more resource than the normal protocols and might be difficult for implementing the security in the existing protocols. This paper uses Information security Principals for classifying the secure multipath routing protocols in wireless sensor network.

A. Wireless Sensor Network Components Security

The wireless sensor network has many components including sensor node, wireless network, transceiver, external memory, power source, Transceiver, base station, management center for store data for analysis. The WSN security achieved only when the solution support end to end security from sensor node to the data center. The sensor data communicate between sensor nodes, communicate between sensor node to base station and base station to the data center. The data use different network topology to communicate between the sensor nodes and different network topology to communicate between the base station and data center. The data should secure in all communication channels. The hardware, software, network and operating system related with sensor node should be secured for secure wireless sensor network.

B. Challenges in WSN security

Many components involved in wireless sensor network which need to be secured. The traditional security system cannot apply directly due resource restriction. The sensor nodes deploy in the hostile environment which may not control directly. Many resource communicated with a sensor node for transmit and receive the data between nodes in sensor networks. It consumes lots of power and bandwidth for communication. The cryptography techniques cannot apply to wireless sensor network which may need a lot of computation. The encryption and decryption cannot apply due to low battery power and low bandwidth [17]. Steganography is another technique used to embed a message into the multimedia data. The wireless sensor network send and receive the multimedia data. But, the sensor devices cannot handle the huge multimedia message for applying stenography.

The existing performance based multipath protocols do not consider the security as a primary goal and vulnerable to attacks. The WSN network attacked by various types of network attacks. The next section discusses more about the various types of attacks in Wireless sensor networks.

III. ATTACKS IN WSN

The wireless network is more vulnerable than wired networks due to the nature [18]. Anyone which has same frequency can monitor and participate in the wireless network. The attacker can be inside the network or outside the wireless network. The attacker receives the important data from Wireless network or attack the network for deactivating the entire network based on the attacker nature. The wireless sensor node deployed in agricultural land, military environment which may not possible to control and monitor the network.

This section discusses with different type of attacks in wireless sensor network:

A. Node capture attacks

The confidentiality and integrity can be compromised by physically capture the sensor node and extract the information from their memory is called Node Capture Attack. This can control the sensor node and use for further attacks.

B. Compromised node

The sensor node deployed in a large number of areas and cannot be monitored. So, the attacker enters in the wireless network and compromise the sensor node. The attacker can get cryptographic keys, information and control the sensor node which part of wireless sensor network.

C. Denial of service (DOS)

The Denial of service (DoS) 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 DoS attack 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 [17].

D. Altering routing Information

Altering routing Information attack the routing information exchanged between nodes. The routing information can alter, spoof or reply by the attacker. The attacker can create routing loops and control the network traffic.

E. Selective forwarding attack

Selective forward attack can drop the network messages and ensure that they are not broadcast further in the network. The malicious nodes act as normal node and drop the messages but drops the messages. The selective forwarding attack is hard to detect.

F. sinkhole attack

The malicious node act as a black hole for attracting all traffic in the nodes [17]. When the malicious node added in the wireless sensor network (between source and sink), it can control the messages passed between the sensor nodes.

G. 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 message selectively [18]. This attack relatively coupled with selective forwarding and Sybil attack and difficult to detect.

H. Sybil attack

The malicious sensor node illegally claims multiple identities. The attacker can generate many sensor node identification using a single physical device [17]. The WSN can use gateway for prevent Sybil type attacks.

I. Byzantine attack

Attack where the system fully controlled by authenticated devices by randomly disrupts the system is called Byzantine attack. It may be Flood Rushing Attack and Black Hole Attack. Black Hole Attack drops the network messages but participate in all wireless sensor networks. Flood Rushing Attack give preference to affected message instead of genuine message.

J. Fabrication attacks

Fabrication attack generates the routing message with false information, resource in the wireless sensor network [10]. An attacker may disturb the network bandwidth and give more traffic to the network. Attacker can attack when the network has less authentication and authorization in the network.

K. Packet-dropping Attacks

Packet dropping attack discards the packet instead of reply the packets in the Wireless sensor network. The Packet dropping is one of the DoS attack.

TABLE I. ATTACK TYPE

SNo	Attack Type	Active	Passive	Mote-Class	Laptop-Class	Insider	Outsider
1	Node capture attacks	X		X			X
2	Compromised node	X		X			X
3	denial of service	X			X	X	X
4	Altering routing Information	X		X			X
5	selective forwarding attack		X	X		X	
6	sinkhole attack	X		X		X	
7	wormhole attack	X		X		X	X
8	Sybil attack	X		X	X	X	
9	byzantine attack	X			X		X
10	Fabrication attacks		X	X	X		X
11	Packet-dropping Attacks	X		X		X	
12	spoof network packets	X					
13	black-hole attack	X		X		X	
14	Hello flood attack		X	X	X	X	

L. *Spoof network packets*

The attacker assumes identify of another node in the network and can send or receive the message. This attack launched before initiate any other attack. The attacker have enough information about the network and gather the information from the network like original node.

M. *Black hole attack*

The malicious node communicates destination node with spoofed route reply information. The destination will send the data to the malicious node in the WSN.

N. *Hello flood attack*

Hello flood attack send the HELLO packet to the sensor node in the wireless sensor network [18]. The sensor may assume the attacked device as a neighbor and try to connect with the WSN. The attacker gets into the wireless network and all the nodes will try to send the HELLO packets to the network which may take a lot of network bandwidth and power.

The security system prevents such attacks in three different approaches. (1) Prevention (2) Instruction Detection and (3) Hybrid. The detection system monitors the system for finding malicious activities and policy violations. It doesn't prevent the malicious activities. The Instruction Prevention system tries to block or stop malicious activities. The Hybrid approach monitor, identify and stop such kind of activities and log the information and report.

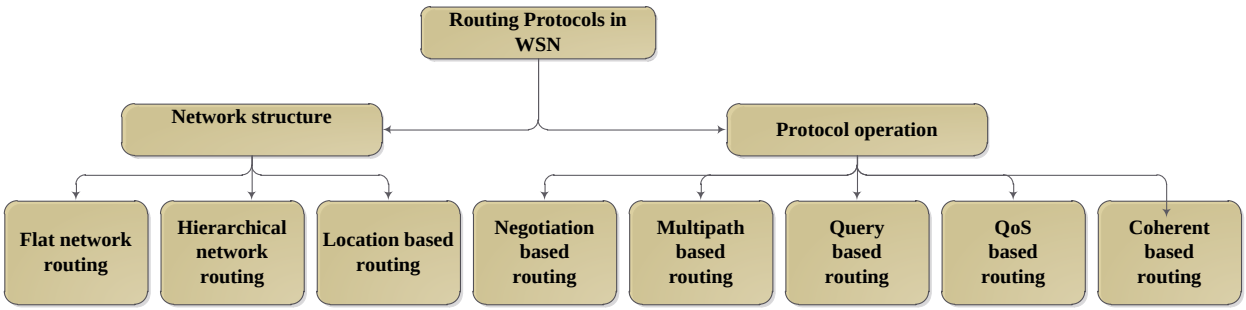

Fig. 1. Rotuing protocol in WSN

IV. WIRELESS SENSOR NETWORKS ROUTING IN WSN

Wireless sensor network has small sensor devices which communicated in the network. The sensor node should communicate with each other using different network topology. The node connects with other sensor node either directly or base station. The routing protocol divided flat based routing, hierarchical based routing and location based routing [20].

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 based routing classified multipath-based, query-based, and negotiation-based, QoS-based, or coherent-based routing techniques depending on the protocol operation. This paper uses multipath routing for analysis about the classification. Fig1 explain the classification of routing protocol in Wireless sensor network.

V. RELATED WORK

The secure multipath routing Protocols in Wireless Sensor Network survey use for security researcher who develop routing algorithms. The researcher can understand the currently available secure routing protocols without spending more time. [12] and [14] analysis secure multipath routing protocols. Ali Modirkhazeni et al. [14] have reviewed with basic security requirement principals Confidentiality, Integrity, Availability and Authentication. It also considers the Key Management and Cryptography Scheme. Finally it generalizes the research about secure multipath routing algorithm and provide the matrix which include all the analysis. Ali Modirkhazeni et al. [13] have provided a survey of Secure Hierarchal Routing Protocols in wireless sensor network. It discusses the information security Basic Security Requirements based on the applications. It also discusses about Sensor device architecture and routing protocols. It concludes with the previous research about the secure hierarchal routing protocols. Eliana Stavrou et al. [12] analysis using information security principals and network attack types and analyzed the various secure multipath routing protocols. This paper extended the concept and discussed secure multipath routing with recent secure multipath routing protocols (from 2010 to 2013).

VI. SECURE MULTIPATH ROUTING PROTOCOLS

Many routing protocols proposed in Wireless sensor network. But, many of the protocols do not consider security while design the protocol and few protocol consider the security. The secure multipath routing protocol does not satisfy all the security principals like normal network. This section analysis the existing secured multipath routing protocol available in wireless sensor network.

A. Attack Types classification

The attack type classification help in understanding the attack types in Wireless sensor network.

1) Passive versus active attacks.

The active attack can modify or alter the data in WSN. The Passive attack monitors the packets in WSN. It will not update or alter any information. The attacker takes the important information which transmitted in wireless sensor network [18].

2) Inside versus Outside attacks.

The insider attack joins the wireless sensor network and act as the internal node. It may have material and other sensor node trust the inside attack node. The inside attack mode is hard to detect. Inside attack can achieve by writing some malicious code in sensor device. The external attack doesn't join in the network and inject the flood attack for consuming the network bandwidth [18].

3) Mote-Class versus Laptop-Class attack

The mote-class attack uses a few sensor nodes with similar capabilities of resources in the network. The Laptop-Class attack uses more powerful resource like a laptop. The Laptop class attack is more powerful attack compare than Mote-class attack.

B. Secure Multipath Routing Protocols classification based on Attack type and Information Security classification

Secure multipath routing protocol survey has been done [12] and [14] with a different point of view using secure multipath routing papers which has been around year 2010. Nowadays, the attacker has more powerful technique and tools available. So, this paper has analyzed the recent attack types and multipath algorithm in wireless sensor networks. Table [2] analysis with Basic security principals, attack type which explained on Table [1] and security operation support.

1) Anri Kimura et al..

The wireless sensor network uses multiple path for routing. Multipath routing uses for different path when the path break and path consume more bandwidth. The single path routing method uses DART. The proposed method extends single path method DART. It uses joint count which is for counting the number of joint nodes and connectedness which uses for finding the maximum degree of path connectedness on the joint node. The proposed method implemented in QualNet simulator and make sure it can detect the node capture attacks without degradation of the data delivery ratio.

2) Tao Shu et al.

Secure Data Collection in Wireless Sensor network proposes the randomized multipath routing algorithm. The route will change for each traversed packet. So, the attacker cannot track all the packet. It's also highly dispersive and energy efficient. This algorithm proposes a three-phase approach for secure information delivery in a WSN; secret sharing of information, randomized propagation and normal routing toward the sink. The proposed randomized algorithm takes more energy consumption compare than the normal routing algorithm. It assumes small number of block holes in the WSN.

3) SCMRP

The secure cluster based multipath routing protocol (SCMRP) use combination of Cluster based routing and multipath routing for getting both benefits. The SCMRP is proactive type protocol which means all the routes are computed before they need. The resource rich base station calculates all the routes. It has five different phases. (1) Detect the neighbor and construct the network topology (2) pairwise key distribution (3) cluster formation (4) data transmission and (5) re-clustering and re-routing.

TABLE II. ASECURE MULTIPATH ROUTING PROTOCOLS CLASSIFICATION

protocol name	Year	Attack Type from Table [1]	Security Operation Support			Basic security principal			
			Prevention	Instruction Detection	Hybrid	Confidentiality	Authentication	Integrity	Availability
Anri Kimura et al. [1]	2012	1	X			X	X	X	
Tao Shu et al. [5]	2010	1, 2	X						X
SCMRP [6]	2010	4, 5, 6, 7, 8			X	X	X	X	X
EENDMRP [7]	2012	4, 5, 6, 8 and 9	X				X	X	
ESRP-M [8]	2011	5		X				X	
NC-RMR [10]	2010	10, 4	X			X			X
IFRP [2]	2011	11			X		X	X	
Arjun P. et al. [3]	2011	11, 12, 13, 14			X	X	X		
SeMuRa [15]	2010	7	X					X	X
MSR [16]	2011	15, 5, 12, 6, 7, 8	X					X	

It helps to reduce the traffic on the network and save energy. The detect the neighbor and construct phase the Base station will verify the MAC for integrity and encrypts the neighbor information using shared key The SCMRP can detect Sybil, Sink hole and Wormhole, Selective forwarding, HELLO flood and Spoofing or altering the route information attacks. The Base station collects all the neighbor list from sensor node and apply the DFS algorithm for finding multiple path. The BS generates the pairwise key and unicast to all nodes. The Cluster head selection is based on the energy of the node Base station monitor the energy in the node and change the routing path.

4) EENDMRP.

Energy efficient node disjoint multipath routing protocol (EENDMRP) uses a Sink initiated proactive secure node disjoint multipath routing protocol and it transmit the data using secure manner by using the digital signature crypto system. The crypto system uses MD5 has a function and RSA algorithm. The RSA algorithm doesn't increase the message size.

Route CONstruction (RCON) packets exchanged between in route construction phase and podcast in the sensor network. The Data Transmission Phase takes node parameters like, the rate of energy consumption, filled queue length and effective residual energy for finding a cost effective primary path between source and destination. EENDMRP climes, it performs better than AOMDV protocol. There is improvement in packet delivery fraction, reduction in end-to-end delay, reduction of normalized routing load and energy saving.

5) ESRP-M.

Efficient and Secure Routing Protocol for Wireless Sensor Networks using Mine detection uses modified the Triple Umpiring System (TUS) by incorporating Mine detection feature. Each node in ESRP-M should play the dual role for packet forwarding and umpiring. The Mine Detection routing algorithm can detect the suspicious behavior in the wireless sensor network. ESRP-M climes that Packet Delivery Ratio (PDR) and End to End Delay improved lot compare than Multipath secure routing protocol for a flat network (MMDP).

6) NC-RMR.

Network coding based reliable disjoint and braided multipath routing (NC-RMR) forms a multiple path maintains only local path information without from the end to end path from source to destination. The NC-RMR protocol divided into five phases (1) calculation of the number of required paths (2) data encoding at the source node (3) next hop node selection and path assignment (4) encoding and transmission at intermediate nodes (5) decoding and data recovery of sink node. This protocol maintains only local routing information without handle the end to end routing information which helps for load balanced and energy efficient.

7) IFRP.

Intrusion/Fault Tolerant Routing Protocol uses single path routing and switch to multipath routing when malicious behavior on the network. It uses a local warden technique to detect and isolate the faulty nodes. This routing algorithm divided in two phases: a new mechanism for creating routing tree and secure routing based on the created tree. TinyOS beaconing protocol use for finding the modified tree from sensor node to base station. The second phase sends the data using first phase. The Modified routing tree generates using Tree generation,

Supplementary parent discovery and Base station and neighbor authentication steps. The Security mechanism based on Local Warden Technique (LWT) use to prevent the packet altering attacks. The second phase uses Routing algorithm for finding the routing information, reliable routing using LWT, Intrusion detection and Intruder Isolation when the node affected.

8) Arjun P. et al..

Towards Secure Multipath Routing for Wireless Mobile Ad-Hoc Networks: A Cross-layer Strategy propose a secure multipath routing mechanism that uses cross layer strategies. The network layer takes the routing decision based on the lower level physical and link layers. The path selection process is based on the forwarding behavior in the sensor network. The node's neighborhood using physical layer measurements uses nodes connectivity information and share

between nodes. The algorithm uses Route establishment and Route management process to establish and manage the routing information. It claims that support reliable and secure multi-path routing via a cross-layer.

9) SeMuRa.

Secure Multipath Routing Algorithm proposes a novel multipath routing algorithm for wireless sensor network. It extended k connectivity to k-x connectivity x is a disjointness threshold representing the maximal number of nodes shared between any two paths in set of k shared paths. The k connectivity makes sure before sending data, a sensor node should make sure the set of k paths available from sensor to Base station. The threshold signature makes secure for this protocol and don't require any other security mechanism. The proposed algorithm extends the Dynamic Source Routing (DSR). The SeMuRa protocol has two phases, route discovery which discovers the multiple path between the nodes and route maintenance which maintain the possible multiple path between the nodes. The nodes may be sensor node or base station.

10) MSR.

A Multipath Secure Reliable Routing Protocol for WSNs propose the secure and reliable multipath routing protocol for wireless sensor network. MSR has three components. On-demand multipath routing, the enhanced passive acknowledgment and erasure coding. The on-demand multipath routing establishes the routing when requires. It don't build the end to end routing information. The on-demand multipath routing has two phases Route request Phase and Route Reply phase. The source node sends ROUTE-REQUEST with source-ID, destination-ID, and request-ID fields and the destination node will send a ROUTE-REPLY message. Multipath routing and erasure coding increase the security. Enhanced passive acknowledge analyze the security behavior passively. The MSR assumes homogeneous network with the same hardware and software, static unique ID. It also assumes the inside mote-class attacker. The MSR claims better than AOMDV, in terms of packet delivery ratio and WSN security attacks.

We have selected secure multipath routing protocols in wireless sensor network with the last three years from 2010 to 2013. In order to generalize the secure multipath routing protocol, we have given the matrix in Table 2. The matrix shows the basic security principles satisfy in Wireless sensor network protocols. It also considers the whether the protocol is used for instruction prevention, detection or hybrid of these two techniques. According to proposed matrix, authentication and integrity are the most satisfied security requirements among selected protocols. The selected multipath protocol doesn't consider much on cryptography with key distribution techniques. Most of the proposed secured multipath protocols prevent one or more attacks. The attack type classified in Table 1. The attack table mapped with each selected multipath protocol in Table 2. When the protocol designed with multipath and security, it may take more power consumption compare than single path routing techniques.

VII. CONCLUSION

In this paper, we have surveyed the secure multipath routing protocols in wireless sensor network. This paper discusses with challenges in wireless senor network security and attacks in WSN. It covers more recent attacks in Wireless sensor network. Other survey papers [12], [13] and [14] analysis the only less number of security attacks in WSN. This paper takes the recent security attacks and give the matrix for active vs passive, Mote-class vs Laptop class, Insider vs. Outsider classification. It also takes the latest secure multipath routing algorithm which uses for detects/prevent the attacks in wireless sensor networks with information security principal and security operation support classification. The proposed matrix can be a basis for the researchers who want to work on the secure multipath routing protocol in wireless sensor network.

REFERENCES

[1] Anri Kimura, Eitaro Kohno, and Yoshiaki Kakuda, "Security and Dependability Enhancement of Wireless Sensor Networks with Multipath Routing Utilizing the Connectedness of Joint Nodes," 2012 32nd International Conference on Distributed Computing Systems Workshops

[2] Hamid Nabizadeh, Maghsoud Abbaspour, " IFRP : An Intrusion/Fault Tolerant Routing Protocol for Increasing Resiliency and Reliability in Wireless Sensor Networks ", 2011 International Conference on Selected Topics in Mobile and Wireless Networking (iCOST).

[3] Arjun P. Athreya and Patrick Tague, " Towards Secure Multi-path Routing for Wireless Mobile Ad-Hoc Networks: A Cross-layer Strategy ", 2011 8th Annual IEEE Communications Society Conference on Sensor, Mesh and Ad Hoc Communications and Networks.

[4] Eitaro Kohno, Tomoya Okazaki, Mario Takeuchi, Tomoyuki Ohta, Yoshiaki Kakuda, Masaki Aida, "Improvement of the Security Against Node Capture Attacks Using Dispersed Data Transmission for Wireless Sensor Networks", 2010 Symposia and Workshops on Ubiquitous, Autonomic and Trusted Computing.

[5] Tao Shu, Student Member, IEEE, Marwan Krunz, Fellow, IEEE, and Sisi Liu, Student Member, IEEE, "Secure Data Collection in Wireless Sensor Networks Using Randomized Dispersive Routes", IEEE TRANSACTIONS ON MOBILE COMPUTING, VOL. 9, NO. 7, JULY 2010.

[6] Suraj Kumar, Sanjay Jena, " SCMRP: Secure Cluster Based Multipath Routing Protocol for Wireless Sensor Networks", 2010 IEEE

[7] Shiva Murthy G, Robert John D'Souza, and Golla Varaprasad, "Digital Signature-Based Secure Node Disjoint Multipath Routing Protocol for Wireless Sensor Networks", IEEE SENSORS JOURNAL, VOL. 12, NO. 10, OCTOBER 2012.

[8] Ganesh Subramanian, Dr.R.Amuth "Efficient and Secure Routing Protocol for Wireless Sensor Networks using Mine detection", IEEE

[9] Zhibin Zhao, Bo Wei, Xiaomei Dong, Lan Yao, Fuxiang Gao, "Detecting Wormhole Attacks in Wireless Sensor Networks with Statistical Analysis", 2010 WASE International Conference on Information Engineering

[10] Yuwang Yang n, ChunshanZhong,YaminSun,JingyuYang, "Network coding based reliable disjoint and braided multipath routing for sensornetworks",Journal of Network and Computer Applications33 (2010)422–432

[11] Haiyong Wang, Geng Yang, Jian Xu, Zhengyu Chen, Lei Chen, Zhen Yang, "A Noval Data Collection Approach for Wirelsee Sensor Networks", 2011 IEEE

[12] Eliana Stavrou, Andreas Pitsillides, "A survey on secure multipath routing protocols in WSNs", Computer Networks 54 (2010) 2215–2238

[13] Ali Modirkhazeni, Norafida Ithnin, Mohammadjavad Abbasi, "Secure Hierarchal Routing Protocols in Wireless Sensor Networks; Security Survey Analysis", IJCCN International Journal of Computer Communications and Networks , Volume 2, Issue 1, February 2012

[14] Ali Modirkhazeni, Norafida Ithnin, Othman Ibrahim, "Secure Multipath Routing Protocols in Wireless Sensor Networks: A Security Survey Analysis", 2010 Second International Conference on Network Applications, Protocols and Services

[15] Bayrem Triki, Slim Rekhis and Noureddine Boudriga, A NOVEL SECURE AND MULTIPATH ROUTING ALGORITHM IN WIRELESS SENSOR NETWORKS

[16] Mariam Ahmed Moustafa, Moustafa A. Youssef, Mohamed Nazih El-Derini, MSR: A Multipath Secure Reliable Routing Protocol for WSNs, 2011 IEEE

[17] Al-Sakib Khan Pathan, Hyung-Woo Lee, Choong Seon Hong, "Security in Wireless Sensor Networks: Issues and Challenges", Feb. 20-22, 2006 ICACT2006

[18] Shio Kumar Singh 1, M P Singh 2, and D K Singh, "A Survey on Network Security and Attack Defense Mechanism For Wireless Sensor Networks", International Journal of Computer Trends and Technology- May to June Issue 2011

[19] C. Karlof and D. Wagner, "Secure Routing in Sensor Networks: Attacks and Countermeasures", Elsevier's AdHoc Networks Journal, Special Issue on Sensor Network (SNPA), Sept. 2003, pp. 293-315

[20] JAMAL N. AL-KARAKI, AHMED E. KAMAL, "ROUTING TECHNIQUES IN WIRELESS SENSOR NETWORKS: A SURVEY", IEEE Wireless Communications • December 2004

AUTHORS PROFILE

Dr. A.Senthilkumar received the MCA Degree from the Madras University, India, in 1999. He received the M.Phil degree in Computer Science, Manonmaniam Sundharnar University, Tirunelveli, India. He received the Ph.D degree in computer applications from Anna University Coimbatore, India. He is Currently Professor in Department of MCA, Sengunthar Engineering College, Tiruchengode, Tamilnadu, India. He has 13 Years and 7 Months of Experience in Teaching. His fields of interest, Computer Networks, Network Security, Wireless Sensor Networks. He Has 15 Publications to his credit in State, National, and International.