STUDY ON ROUTING PROTOCOLS FOR THE SECURITY OF WIRELESS SENSOR NETWORKS

Aditya Kulkarni (Student) and Kurt Kosbar (Advisor)
Telemetry Learning Center
Department of Electrical and Computer Engineering
Missouri University of Science and Technology

ABSTRACT

This paper describes some of the security challenges faced by Wireless Sensor Networks (WSN). A classification and analysis of prominent attacks on the routing protocols of WSN is provided, along with a review of recent developments in the field to help mitigate the impact of these attacks

Keyword: wireless sensor networks, routine, secure communications

INTRODUCTION

New innovations in wireless ad hoc networks, battery technology and solid state electronics have increased the scope of application of wireless sensor networks (WSN). They are used in diverse applications including Environment Observation and Forecasting Systems and Structure Health Monitoring Systems. They are suitable for military use for battlefield surveillance, targeting, damage assessment and biological attack detection [1]. These developments demand novel schemes to be associated with WSNs for enhanced performance and reliable security. Consequently trustworthiness and security of these systems become the basic design concern.

A step towards this direction is the development of novel secured routing protocols. Several routing protocols are designed to specifically thwart the effects of widely recognized attacks. A systematic study shows that they are based on unconventional methods and are a result of novel concepts. This work provides an investigation of secured routing schemes.

Section II provides a background to our study. In section III we classify the prominent attacks on routing protocols of WSNs. In section IV we discuss countermeasures to these attacks. In section V we note the recent developments and upcoming trends and section VI concludes our study.

BACKGROUND

Incorporation of security features typically involves introduction of data redundancy and mathematical operations such as encryption and decryption. Such operations demand additional power, processing speed and memory. However WSNs are severely limited on most of the resources. Therefore it is relevant to examine the limitations of WSNs that will allow a judicious

choice of the security protocol. In view of this requirement this section provides an overview of the prominent constraints in WSNs that can affect the feasibility of implementation of a security protocol.

ATmega128L and MSP430 are commonly used processors in WSNs. ATmega128L is a low-power microcontroller with 128KB memory and 4KB RAM [3]. MSP430 is an Ultra-Low-Power microcontroller with 512KB memory and 64KB RAM [4]. The highly limited memory and RAM indicate the need for compact, robust security algorithms that are less demanding on memory. In [2] an account on the specifications of the prominent systems used in WSNs is seen.

Energy is one of the most limited resources available at the nodes of a WSN. In the applications where WSNs are deployed in unattended environments, it may not be practical to recharge the batteries during operation. Basic functionality of WSNs includes transmission, reception and storage of data that are process that consume noticeable amounts of energy. This requirement has motivated innovation in battery technology [5] and new energy management schemes [6]. It is critical that the security algorithms associated with WSNs are highly energy efficient with minimum computations and using very limited amounts of memory.

The unreliable communication in WSNs is associated with loss and damage to the data packets and is susceptible to attacks. This adds additional challenges in ensuring the secured performance of the WSNs. The choice of routing protocols determines the reliability of communication. Also, it is often required that the chosen protocol has features that provide immunity to variety of attacks.

ATTACK ON WSNs

The types of attacks that affect WSNs are unique. There is a wide scope for attacks since the WSNs operate in hostile environments. The common attacks that target the routing protocols are included in one of the following classifications [7]

Spoofed or altered routing information

Routing information typically includes source address, destination address, next hop location, hop limit, data-type, etc. Unauthorized alterations of these fields can severely reduce the performance of the network. Formation of network loops, routing through sub-optimal paths, network partition, traffic congestions, undesired repelling of the traffic and increase in end-to-end delay are some of the common consequences of this attack [8].

Sinkhole attacks

Sinkhole is a compromised node that attempts to attract traffic through itself by broadcasting fake information of identity to alter, drop or analyze the data packets. The effect of this attack is more pronounced in proactive routing protocols that develop the routes on the go. A sinkhole attracts packets through all of its neighboring nodes and creates a region of high data density in the network. A single sinkhole node is known to attract significant amount of traffic to an extent that the entire network is compromised. A typical method of sinkhole attack is discussed in [10].

Selective forwarding attack

When a malicious node selectively drops packets it is identified as selective forwarding attack. The communication link between the nodes of the WSNs is unreliable. Consequently a certain loss of packets during transfer is expected. This makes detection of selective forwarding attack challenging. Selective forwarding attack in combination with sinkhole attack is seen to be highly effective in disrupting the operation of many routing protocols such as TinyOS beaconing, directed diffusion, GPSR, GEAR [13]. Figure 1 and figure 2 demonstrate the possible cases of selective forwarding attack [14].

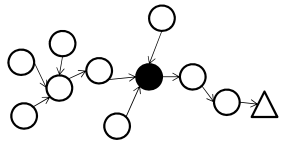

Figure.1 Selective forwarding attack with single malicious node

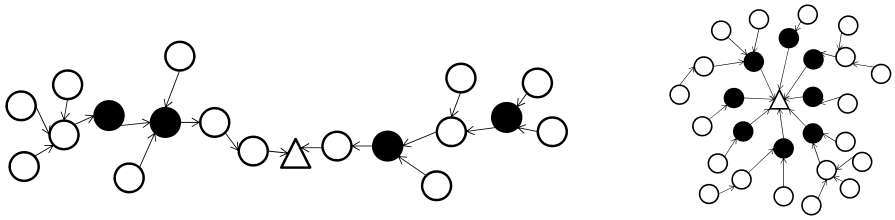

Figure.2 Selective forwarding attack with multiple malicious nodes

Sybil attack

A single compromised node appears to be different nodes at different instances of time. Reference [18] discusses the following common consequences of Sybil attack:

1. Distributed storage: Replication of data is a common feature in WSN. In case of Sybil attack this architecture is disturbed since the data is stored in fake identities generated by a single node.

2. Routing: Powerful routing techniques such as multipath routing and geographic routing are ineffective in fighting Sybil attack since the multiple paths may essentially be routed through a single Sybil node.

3. Data aggregation: Due to lack of resources in WSNs certain nodes are assigned to aggregate and store data. The Sybil node can store junk information posing as a new user many times and thereby depleting valuable resources

4. Voting: In WSNs a method of voting to take a decision is often seen. Sybil attack can easily control the outcome of posting fake votes in disguise of many nodes.

5. Misbehavior detection: Several schemes and principles are implemented to detect misbehaving nodes. The Sybil nodes can manipulate such schemes that can render the network to be incompetent of intrusion detection.

6. Attack on VANETs: Vehicular Ad Hoc Networks (VANETs) are used to determine critical traffic information. A Sybil attack on VANETs can project illusion of false traffic or traffic congestion. This can have serious impacts that can be detrimental to passengers of a vehicle.

The Sybil attack is known to reduce effectiveness of distributed storage, dispersity and multipath routing and topology maintenance [8]

Wormholes

Reference [20] provides an elegant description of wormhole attacks. Consider a malicious node A that tunnels packets to another malicious node B and node B replays the packet in the network. This creates an illusion of a short path usually of one or two hops between node A and node B. Such a pair attracts significant traffic in the network. This setup forms the premise for attacks such as selective forwarding attack or eavesdropping. Deployment of wormholes at strategic locations can make this attack extremely effective. For instance if a node in the proximity of a base station forms a wormhole pair with another malicious node the whole routing may be disrupted [8]. Wormhole attacks can be designed to prevent discovery of desired routes or disrupt the functioning of an established route and cause selective forwarding attack which qualify as instances of Denial of Service. They can also hinder the functioning of the access control systems [21].

HELLO flooding attack

In wireless ad hoc networks it is required that the nodes exchange information so that every node in the network knows the other reachable nodes. A common method to broadcast the existence of a node in a network is by flooding HELLO packets. Routing protocols allow periodic broadcast or event driven broadcast of HELLO packets. When node B receives a HELLO packet from node A, node B assumes that node A is within its transmission range. A laptop class adversary can use this fact to flood the network with fake HELLO packets of considerable signal strength. The nodes assume adversary to be a neighbor while in essence they are separated by several hops. Therefore packets routed to the adversary are deviated away from the actual destination. Effectively every route can get directed towards the adversary and the network will be compromised. HELLO flooding attack is a major threat since it is easy to implement and highly effective in disrupting the reliability and performance of the entire network. [8, 22]

COUNTERMEASURES

Spoofed or altered routing information

Spoofing the routing information is a direct attack on the routing protocol that can quickly degenerate the network. Eavesdropping, data modification and MAC spoofing are some attacks that can be classified in this section. It is a fundamental objective to gain immunity from such attacks to ensure privacy, reliability and trustworthiness of the sensor networks. To implement such a system the routing protocols must include security mechanisms that offer data integrity, confidentiality, availability and key management. The classical methods of cryptography have to be modified and enhanced to meet the special challenges associated with WSNs. Further the design of security architectures depends on application of WSNs. It is noticed that that the Medium Access Protocols such as CSMA, polling, token ring or RTS/CTS are susceptible to

attacks, for example the attacker may flood duplicate RTS (Request To Send) and CTS (Clear To Send) packets. An approach to address this problem has been development of routing protocols in augmentation with broadcast authentication protocols, for example TESLA (Timed Efficient Stream Loss-tolerant Authentication) and Ariadne [9].

The key generation and distribution is a critical part in development of secured routing schemes. It is seen that asymmetric key ciphers that use clock synchronization and delayed key disclosure methods are developed for this purpose. A one-way key chain is generated by repeatedly computing hash functions using robust methods such as Coppersmith and Jakobsson method.

Some general concepts involved to make the process of routing immune to spoofing attacks includes limiting the maximum number of hops, use of MAC and digital signatures for authentication and non-repudiation and use of control packets to indicate transmission, reception or error in routing. It may be relevant at this point to analyze the features of a control packet. Fig.2 shows different fields of an error control packet.

Error Number	Sender Address	Receiver address	Time to destination	MAC of the previous fields	Key

Figure.2 Error control packet

The error packet is seen to have six fields. The first field has an error number that suggests the kind of error encountered. The address of a node that fails to send the packet is allotted the second field. The address of a node that fails to receive the packet is allotted the third field. The remaining fields ensure security. The fourth field has an estimate of the maximum time that an error packet may take to reach the source. This will ensure the fake packets to be discarded. MAC is used for authentication. The final field allows intermediate nodes to evaluate the error packet. This idea has been conceived in [9].

Sinkhole attacks

Use of SNR and received signal energy metrics is a common method for detection of sinkholes. The instances of this method are discussed in this section. Link Quality Indicator (LQI) based routing protocols such as LOAD (6LoWPAN Ad Hoc On-Demand Distance Vector Routing) are highly suitable for WSNs. Choi et al. [11] has developed sinkhole detection scheme for LQI based routing for WSNs. LQI is a reactive protocol with two stages – route discovery and route maintenance.

These processes need to be immune to sinkhole attack. In route discovery stage sinkhole can alter the LQI tables that note link cost between nodes to route the traffic through itself and during route maintenance it transmits strong control signals requesting for data packets. Detector nodes are used maintain a path cost table between other detector nodes that notice illegal alterations in the LQI tables. Fake control packets issued by the sinkhole are detected with use of the LQI tables maintained at every node.

Ad-Hoc On Demand Vector (AODV) is another common routing protocol used in WSNs. A simple four stage secured AODV is proposed in [10]. The routes are established in the

initialization phase and are stored in the storage phase. The following investigation stage is for security that allows comparison of the routes developed with the previous ones to check for aberrations followed by a resumption phase that resumes the operations of the default AODV. A generic approach to security against sinkhole attacks is given by Tumrongwittayapak et al. [12] that records security algorithms that use trust scheme applied to a routing protocol and construction of a network flow graphs. They present a new scheme uses Extra Monitor (EM) nodes associated with the base node to eavesdrop all traffic to record Received Signal Strength Indicator (RSSI) for source and destination pairs to create a Visual Geographic Map (VGM). The RSSI is compared with those calculated during the initialization of the network for detection of sinkholes.

Selective forwarding attack

Resistance to selective forwarding attack can be realized in two ways that are multipath based schemes and node detection based schemes that are discussed in this section.

Multipath based schemes

A prevalent scheme to thwart variety of attacks is by multipath routing that offers security by including sufficient redundancy. Reference [15] develops algorithms for two types of multipath networks namely, disjoint multipath and braided multipath. In disjoint multipath scheme the sink develops a series of routing requests to neighboring nodes that are sequenced based on the performance of the particular node. The multiple paths thus developed do not include any common nodes.

The most efficient path is called the primary path. In braided multipath scheme the intermediate nodes issue request for alternate routes and new routes branch out through the primary path. Disjoint paths can provide better security but have greater overhead in comparison with braided multipath scheme. Although multipath schemes are attempted to be energy efficient they are associated with considerable overhead. Moreover they are incapable of detecting the launch of selective forwarding attack.

Node detection based schemes

These concerns have led to the development of schemes that can detect malicious nodes and exclude them from routing paths. A common technique is use of watermarking to WSNs. Such a scheme is realized in [16]. Every node is dynamically assigned a trust value based on measure of its honesty to the network. When the network is initiated all every trust value is initialized to a common number. Throughout the operation of the network the trust values are increased (linearly) or decreased (exponentially) based on the performance of nodes. Usually multi-hop algorithms attempt to find the shortest path between the source and the sink that may not be the most secured path. However the current scheme determines optimal path between source and sink based on trust value and geographical location of the nodes. Once these paths are established the watermarked packets the offer confidentiality and authentication are communicated.

The watermarking enables detection loss and juggling of packets. If the base station (sink) suspects selective forwarding attack through a path, it sends back a watermarked packet through this path. The intermediate nodes compare the received packet with the one generated according

to a proposed algorithm [16] to determine net loss of packets at the previous node. If the loss is greater than loss due to unreliable link the trust value of the corresponding node is decreased. It may be relevant to note that even if a node is suspected to be malicious it is not rejected from the network. The trust value is designed to increase linearly in times of reliable performance of a node.

Reference [17] discusses CHEMAS and presents CADE (Cumulative Acknowledgement based DEtection) that are acknowledgment based special secured routing protocols to thwart selective forwarding attack.

Sybil attack

The following list provides a summary of the description of prominent security schemes used against a Sybil attack [19].

1. Radio resource testing: is a novel method of direct detection that involves sounding of message through unique channel to each of the neighboring nodes. The Sybil node fails to hear the message in its dedicated and hence can be detected

2. Random key redistribution: This method is built on the concept that each node is randomly assigned with key-related information that is used to compute the shared pair of keys. It is also considered that the network can validate these keys for identification of a node.

3. Registration: WSNs include a central authority (CA) to manage the network. The CA maintains a register of well-behaved nodes and malicious nodes. The CA can initiate network polling and compare the results with the registers to identify Sybil attack. However it must be ensured that the node deployment information maintained by CA is secured.

4. Position verification: The physical location of a node is verified by the network. This technique is seen to be relatively new with wide scope for improvement.

Many powerful Sybil attack detection scheme are designed to localize the Sybil node by measurement of RSSI (Received Signal Strength Intensity) [18]. Different methods are developed to allow the nodes to measure RSSI and cooperatively detect the Sybil node. A special technique for VANETs is also discussed. It involves statistical treatment on signal strength distribution received from a suspicious vehicle. Every vehicle plays the role of "claimer, witness and verifier" at different occasions. The verifier checks the location of the claimer based on the statistical analysis of signal strength distribution obtained from the witness (neighboring vehicles of claimer). MMSE (Minimum Mean Square Error) method is used to obtain an optimal estimate of the position of the claimer. If the position detected through this method is seen to be varying by a margin from the claimed position the claimer is classified as a Sybil node.

Wormhole attack

A variety of approaches to detect wormhole attack can be seen in literature. In multi-hop networks such as WSNs some schemes allow use of connectivity graph that represents network topology. A connectivity graph is used to detect forbidden sub-networks that may form a

wormhole. Wormholes can also be detected based on a RTT (Round Trip Time) metric that consists of the round trip time required between a node and its neighboring nodes that constitute part of a legitimate route.

A hop-count based system called Wormhole Geographic Distributed algorithm is also seen. It is critical that detection of wormhole attacks is followed by systems to thwart its effects. A digital investigation based system to counter wormhole attack is studied. The algorithm designates special nodes called "observers" to the network that monitors the datagrams, their routes and identifies suspicious nodes. The base station is associated with algorithm to process these data that are securely forwarded to it by the observers to identify the wormhole attacks. These facts are realized from [21].

HELLO flooding attack

A solution to HELLO flooding attack is development of authenticated link between the nodes that support encryption of data. Such a system is developed in [22]. It is based on two founding ideas: sharing if additional secret information to establish pairwise key between nodes and use of multipath multi-base station routing protocols. The key generation scheme proceeds as follows. The initial secret information assignment is based on a multiple tree structure shown in figure3.

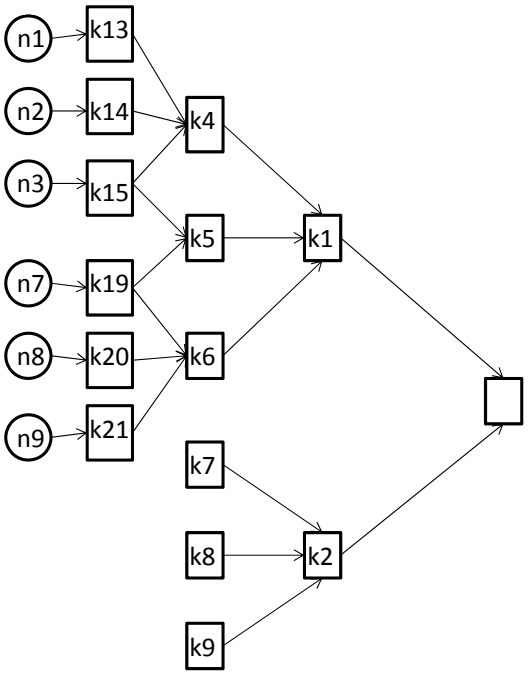

Figure.3 [22] Tree structure for key assignment

At each level every node obtains the secret information of "siblings of its ancestors". Two nodes identify the least common ancestors while they establish communication. For instance if n1 and n3 want to communicate they use k14 and if n1 and n7 want to communicate they use k5. Further they establish that with maintenance K uncorrelated trees the probability that the security is breached is $(2/((d+1))^{K})$ where d represents the degree of the tree. Let us assume that two

nodes share n secret information between them. During establishing a communication the nodes compute MAC of a part of this set of shared secret information to generate a new key. The receiver calculates the MAC of the message to confirm the key ID of the sender and authenticates the message. The authors suggest use of RC5 symmetric cipher algorithm for computation of the MAC. Such a scheme that allows the keys to be generated on the go provide good security against HELLO flooding attack. Their scheme also augments multi-path multi-base propagation scheme that greatly increases reliability of the network

RECENT DEVELOPMENTS

The need for larger and more robust networks has propelled development of new routing protocols. These protocols are designed to enhance the efficiency while offering meticulous security. Development of learning algorithms and energy aware schemes are interesting examples of the new trend.

Most of the learning algorithms are based on use fractional data and feedback. The route discovery methods are upgraded to record all possible routes between source and destination. The packets is divided and communicated through distinct routes. A feedback is obtained to assess the performance of these individual paths. This allows dynamic allocation of data to ensure maximum efficiency. It is evident that such a scheme will induce sufficient randomness in routing. Moreover the data is split arbitrarily among many routes. These factors provide excellent immunity against attacks. Such a method eliminates the need for watchdog nodes and use of special nodes to monitor the health of the network. The absence of such a hierarchy among nodes makes the network immune to blackmail attack and wrong black listing attacks. An example of such a scheme is flow oriented routing protocol. They find routes on demand by using the trends of present flow of data through different routes [23].

The traditional routing schemes are designed to communicate through optimal paths. It is seen that the WSNs are lean on resources. Such a scheme rapidly depletes the resources of nodes along the optimal paths. Further, it makes the system highly predictable. It is relevant to note that all packets are sent through a single path. These factors make routing protocols highly vulnerable to attacks. Energy aware algorithms are developed to counter these problems. Sufficient intelligence is introduced in such schemes that allow arbitrary use of sub optimal paths. This ensures uniform decay of resources throughout the network while introducing randomness to thwart attacks. The problem of network partitioning is also catered by such a method [24].

Algorithms that adopt suitable routing technology for the nodes in accordance with the distance of nodes to the base station, node distribution and energy of nodes are being developed. Such an algorithm that can balance varying concerns among different demand situations by selecting suitable threshold value offers interesting security features [25].

Hybrid protocols are a strong topic of research in the recent times. They combine the advantages of proactive and reactive routing protocols. Until the traffic builds up to a threshold the routes are established proactively and later additional nodes are activated that are serviced through reactive flooding [26].

A self-optimized and autonomous secure routing mechanism: Biological inspired self-organized Secured Autonomous Routing Protocol (BIOSARP) that is based on Ant Colony Optimization technique (ACO) [27] and cost effective solutions [28] are the accounts of recent developments.

CONCLUDING REMARKS

It is evident that WSNs are deployed in variety of environments and are exposed to an exhaustive set of attacks owing to their hostile environment and structural limitations. Consequently design of a secure WSN is a highly challenging task. Analysis of security of WSNs is highly complex. A reliable choice of scheme for these systems needs a firm and clear foundation. This work is a step towards providing such a framework and hence can be considered to be a good contribution in the area of security of WSNs.

REFERENCES

[1] Chee-Yee Chong; Kumar, S P., "Sensor Networks : Evolution, opportunities and challenges", Proc IEEE, August 2003.

[2] Mark Hempstead, Michael J. Lyons, David Brooks, and Gu-Yeon Wei; "Survey of Hardware Systems for Wireless Sensor Networks"; Journal of Low Power Electronics Vol.4, 1–10, 2008

[3] Datasheet ATMEL ATmega128L (http://www.atmel.com/Images/doc2467.pdf)

[4] Datasheet Ultra-Low-Power MSP430™ Microcontrollers (http://www.ti.com/lit/sg/slab034v/slab034v.pdf)

[5] Chulsung Park, Kanishka Lahiri, Anand Raghunathan; "Battery Discharge Characteristics of Wireless Sensor Nodes: An Experimental Analysis", Sensor and Ad Hoc Communications and Networks, IEEE SECON 2005, Publication Year: 2005 , Page(s): 430 – 440.

[6] Hengyu Long, Yongpan Liu, Yiqun Wang, Robert P. Dick, Huazhong Yang, "Battery Allocation for Wireless Sensor Network Lifetime Maximization Under Cost Constraints", ICCAD '09 International Conference on Computer-Aided Design, 2009, Pages 705-712

[7] Shashikala, Dr. Kavitha.C; "A Survey on Secured Routing Protocols for Wireless Sensor Network", 2012 Third International Conference on Computing Communication & Networking Technologies, 2012 , Page(s): 1 - 8

[8] Chris Karlof, David Wagner, "Secure routing in wireless sensor networks: attacks and countermeasures, Ad Hoc Networks", Volume 1, Issues 2–3, sept 2003, Pages 293–315

[9] Yih-chun Hu, "Ariadne: A secure on-demand routing protocol for ad hoc networks", Journal Wireless Networks archive Volume 11 Issue 1-2, January 2005 Pages 21-38

[10] Gandhewar, N. ; Patel, R.; "Detection and Prevention of Sinkhole Attack on AODV Protocol in Mobile Adhoc Network"; Fourth International Conference on Computational Intelligence and Communication Networks (CICN), 2012 , Page(s): 714 - 718.

[11] Byung Goo Choi, Eung Jun Cho, Jin Ho Kim, Choong Seon Hong and Jin Hyoung Kim; "A Sinkhole Attack Detection Mechanism for LQI based Mesh Routing in WSN", International Conference on Information Networking, 2009, Publication Year: 2009 , Page(s): 1 - 5

[12] Tumrongwittayapak, C. ; Varakulsiripunth, R.; "Detecting sinkhole attack and selective forwarding attack in wireless sensor networks"; 7th International Conference on Information, Communications and Signal Processing, 2009 , Page(s): 1 - 5

[13] Guorui Li ; Xiangdong Liu ; Cuirong Wang; "A sequential mesh test based selective forwarding attack detection scheme in wireless sensor networks" International Conference on Networking, Sensing and Control (ICNSC), 2010 , Page(s): 554 - 558

[14] Hung-Min Sun ; Chien-Ming Chen ; "Ying-Chu Hsiao, An efficient countermeasure to the selective forwarding attack in wireless sensor networks", 2007 , Page(s): 1 - 4

[15] Deepak Ganesan, Ramesh Govindan, Scott Shenker, Deborah Estrin; “Highly-resilient, energy-efficient multipath routing in wireless sensor networks”, 2nd ACM international symposium on Mobile ad hoc networking & computing, Pages 251-254, 2001
[16] Huijuan Deng ; Xingming Sun ; Baowei Wang ; Yuanfu Cao; “Selective forwarding attack detection using watermark in WSNs”; ISECS International Colloquium on Computing, Communication, Control, and Management, 2009. CCCM 2009, Page(s): 109 - 113
[17] Young Ki Kim, Hwaseong Lee, Kwantae Cho, and Dong Hoon Lee; “CADE: Cumulative Acknowledgement based Detection of Selective Forwarding Attacks in Wireless Sensor Networks”, Third International Conference on Convergence and Hybrid Information Technology, 2008. ICCIT '08,2008 , Page(s): 416 - 422
[18] Abbas, S. ; Merabti, M. ; Llewellyn-Jones, D., “Signal Strength Based Sybil Attack Detection in Wireless Ad Hoc Networks”, 2009 Second International Conference on Developments in eSystems Engineering (DESE), 2009 , Page(s): 190 - 195.
[19] Newsome, J. ; Shi, E. ; Song, D. ; Perrig, A., “The Sybil attack in sensor networks: analysis & defenses”, Third International Symposium on Information Processing in Sensor Networks, 2004, Page(s): 259 - 268
[20] Jin Guo ; Zhi-yong Lei; “A kind of wormhole attack defense strategy of WSN based on neighbor nodes verification”; 2011 IEEE 3rd International Conference on Communication Software and Networks (ICCSN), 2011 , Page(s): 564 - 568
[21] Triki, Bayrem ; Rekhis, Slim ; Boudriga, N.; “Digital Investigation of Wormhole Attacks in Wireless Sensor Networks; Eighth IEEE International Symposium on Network Computing and Applications”; 2009 , Page(s): 179 - 186
[22] Hamid, A. ; Mamun-Or-Rashid ; Choong Seon Hong, “Defense against lap-top class attacker in wireless sensor network”, The 8th International Conference on Advanced Communication Technology, 2006, Page(s): 5 pp. – 318
[23] Meghanathan, N.; DeMarcus, T.; Addison, E.S; “Multicast extensions to the Flow-Oriented Routing Protocol and Node Velocity-based Stable Path Routing Protocol for Mobile Ad hoc Networks”; International Conference on Ultra Modern Telecommunications & Workshops, 2009. ICUMT '09.
[24] 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, 2012 , Page(s): 2941 - 2949
[25] Hongbing Cheng, Chunming Rong, “Design and analysis of a secure routing protocol algorithm for wireless sensor networks”, 2011 International Conference on Advanced Information Networking and Applications, Page(s): 470 - 473
[26] Khatkar, A.; Singh, Y; “Performance; Evaluation of Hybrid Routing Protocols in Mobile Ad Hoc Networks”; 2012 Second International Conference on Advanced Computing & Communication Technologies (ACCT)
[27] Saleem, K. ; Fisal, N.; Enhanced Ant Colony algorithm for self-optimized data assured routing in wireless sensor networks, 18th IEEE International Conference on Networks (ICON), 2012 , Page(s): 422 - 427
[28] Christina, D.P.S.E.; Chitra, R.J., Energy efficient secure routing in wireless sensor networks, 2011 International Conference on Emerging Trends in Electrical and Computer Technology (ICETECT), Publication Year: 2011 , Page(s): 982 – 986