ISSN:0975-9646

Survey of Detection of Sinkhole Attack in Wireless Sensor Network

Kesav Unnithan S L[#1], Lakshmi Devi C*[2] , Sreekuttan Unnithan C[#3]

[#1]*Department of Computer Science and Engineering*
Cochin University of Science and Technology , Thrikakkara Cochin 682022 Kerala India

[*2]*TANGEDCO*
Anna Salai Chennai 600002 Tamil Nadu India

[#3]*Department of Humanities and Sciences,*
Dr. M G R Educational and Research Institute, University
Maduravoyal Chennai 600095 Tamil Nadu India

***Abstract*— Wireless Sensor Network (WSN) is emerging as a prevailing technology due to its wide range of applications in military and civilian domains. These networks are easily prone to security attacks. Unattended installation of sensor nodes in the environment causes many security threats in the wireless sensor networks. There are many possible attacks on sensor network such as selective forwarding, jamming, sinkhole, wormhole, Sybil and hello flood attacks. Sinkhole attack is among the most destructive routing attacks for these networks. It may cause the intruder to lure all or most of the data flow that has to be captured at the base station. Once sinkhole attack has been implemented and the adversary node has started to work as network member in the data routing, it can apply some more threats such as black hole or grey hole. Ultimately this drop of some important data packets can disrupt the sensor networks completely. This paper focuses on the various methods that can be implemented to overcome this attack likeLocation Based Compromise Tolerant Security Mechanism, Hop Count Monitoring Scheme and through Non Cryptographic Method of Sinkhole Attack Detection.**

***Keywords*— -- Wireless Sensor Network, Sinkhole attack, Hop Count Monitoring Scheme, Non Cryptographic Method**

I. INTRODUCTION

Wireless sensor networks (WSNs) have emerged as one of the important technologies for the future. They have numerous potential applications which include environment monitoring, health monitoring, and military applications among others. WSNs typically consist of small and inexpensive devices deployed in open, unprotected, and unattended environments for long term operations to monitor and collect data. This data is subsequently reported back to the base station over a wireless link. The WSN is vulnerable to various attacks; hence security is an important factor in the design of WSNs. However, sensor nodes have limited memory, power, computational capability, and transmission range. Therefore, the limited resources nature of sensor networks posts a great challenge to any proposed security solution. Security solutions for WSNs can be categorized into two main categories: prevention-based and detection based. Prevention-based approaches use techniques such as encryption and authentication which are not practical for WSNs because of their high computational complexity. In addition, the use of broadcasting medium for transmission makes these techniques inappropriate as the attacker may get access to the encryption keys easily. Detection-based approaches use techniques that are able to identify attacks based on the system's behaviour. WSNs can be categorized into two types based on the nodes' capabilities: homogeneous WSNs where every sensor node has the same capability; and heterogeneous WSN where some of nodes have greater capabilities (such as longer transmission range).

II. WIRELESS SENSOR NETWORK PARAMETERS

1. Scalability to large scale of deployment.
2. Heterogeneity of nodes.
3. Mobility of nodes.
4. Power consumption constraints for nodes using batteries or by energy harvesting.
5. Ability to cope with node failures.

III. ATTACK ON WIRELESS SENSOR NETWORKS

A. Sinkhole Attack

In a sinkhole attack an intruder compromises a node or introduces a counterfeit node inside the network and uses it to launch an attack. The compromised node tries to attract all the traffic from neighbour nodes based on the routing metric used in the routing protocol. When the compromised node manages to achieve that, it will launch an attack.

Sinkhole attacks are a type of network layer attack where the compromised node sends fake routing information to its neighbours to attract network traffic to itself [2]. Due to the ad hoc network and many to one communication pattern of wireless sensor networks where many nodes send data to a single base station, WSNs are particularly vulnerable to sinkhole attacks[3]. Based on the communication flow in the WSN the sinkhole does not need to target all the nodes in the network but only those close to the base station.

We consider two scenarios of sinkhole attacks. In the first the intruder has more power than other nodes. In the second the intruder and other nodes have the same power. In both cases the intruder claims to have the shortest path to base station so that it can attract network traffic. In a wireless sensor network the best path to the base station is the basic metric for routing data.

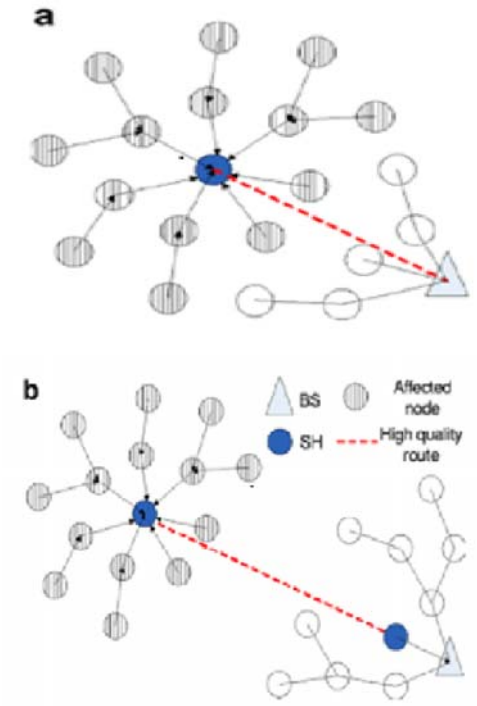


Fig.1. Two illustrations of sinkhole attack in WSN a) using artificial high quality route b) using worm hole [4]

In Fig 1(a)the intruder has greater computational and communication power than other nodes and has managed to create a high quality single hop connection with the base station. It then advertises its high quality routing message to its neighbours. After that all the neighbours will divert their traffic to the base station to pass through the intruder and the sinkhole attack is launched.

In Fig 1(b) the sinkhole attack is launched in conjunction with a wormhole attack. This attack involves two compromised nodes linked via a tunnel or wormhole [2].

IV. Mechanism for Overcoming Sinkhole Attack

A. *Location-Based Compromise-Tolerant Security Mechanism*

Many WSNs have an intrinsic property that sensor nodes are stationary, i.e., fixed at where they were deployed. This property has played an important role in many WSN applications such as target tracking [6] and geographic routing [7]. By contrast, its great potential in securing WSNs has so far drawn little attention. Based on this observation, Zhang proposed a suite of location-based compromise-tolerant security mechanisms for WSNs.

To mitigate the impact of compromised nodes in WSN's, a Location-Based Compromise-Tolerant Security Mechanism[5] implements the notion of location-based keys (LBKs),based on a new cryptographic concept called pairing, for binding private keys of individual nodes to both their IDs and geographic locations. LBK-based neighbourhood authentication scheme is then developed to localize the impact of compromised nodes to their vicinity. It introduces an efficient approach to establish pair wise shared keys between any two nodes that are either immediate neighbours or multi hop away. Such keys are fundamental in providing security support for WSNs. This approach features low communication and computation overhead, low memory requirements, and good network scalability.

LBKs can act as efficient countermeasures against some notorious attacks against WSNs. These include the Sybil attack [8], [9], the identity replication attack [9], wormhole and sinkhole attacks [8], and so on. Finally a location-based threshold-endorsement scheme, called LTE, is used to thwart the infamous bogus data injection attack, in which adversaries inject lots of bogus data into the network. Conclusively, there are enormous potential applications of LBKs in WSNs, such as misbehaviour detection, secure distributed storage, secure routing, and target tracking.

B. *Hop-Count Monitoring Scheme*

To detect sinkhole attacks, we require an intrusion detection system (IDS) that recognizes abnormal route updates. Route advertisements from an attacker syntactically appear as legitimate advertisements, hence we cannot use a misuse [10] or signature based detection system. To address this problem, an anomaly detection scheme is used to detect abnormal route advertisements that are caused by sinkhole attacks. This approach to detecting abnormal route advertisements is to monitor the advertised hop-count values. A significant change in the hop-count value is an indication of the presence of a sinkhole attack. A key research challenge in this approach is how to detect abnormal hop count values in a computationally efficient way within the resource constraints of wireless sensor nodes.

In this schema, Daniel Dallas proposed an Anomaly Detection System (ADS) [11] in which the sinkhole detector was designed so as to discover an observable feature that reacts to the attack in a consistent manner so that it can be used to reliably trigger an alert.

To create a sinkhole, the attacker needs to understate its distance, which is accomplished in distance vector routing protocols by claiming a low hop-count – representing a short distance. With hop-count forgery playing an intrinsic role in the success of a sinkhole attack, it was analysed whether forged hop-counts would be conspicuous enough to reliably indicate the presence of an attack. It was found that physically static nodes have indicated that a reduction in hop-count will not occur except as a result of forging the hop-count value. Also evident was that when efficient routes are created from base station advertisements, large increases in hop-count are unlikely to occur simply due to traversing a slightly different set of nodes. Abnormally large increases in hop-count resulted from an abnormal route detour, which was likely to have occurred due to a failure in the more efficient path.

Therefore this schema watches for attacks when the hop count shifts abnormally low and watches for failures when the hop-count shifts abnormally high. Consequently, all variations in hop-count for anomalies were scrutinized, and the resulting IDS imposes thresholds on hop-count variation (representing variation in distance) when routing paths are updated. Hop-counts below the lower threshold become suspect attacks and hop-counts above the upper threshold indicate the failure of multiple nodes.

Another challenge in the design of this intrusion detection scheme is where to locate the ADS in the network. Given the resource constraints of wireless nodes, it is important to avoid deploying the ADS on all nodes in the network. An alternative solution would be to deploy the ADS at the base station, and monitor the consistency of traffic arriving at the base station. However, a sinkhole attack can effectively disguise its presence – preventing detection from an ADS located at the base station – by restricting its broadcast so that the ADS does not hear the attack. The sinkhole can then forward all traffic through a wormhole to the base station. Consequently, this IDS can be deployed at multiple strategic locations in the sensor network in a decentralized manner.

Since the hop-count feature is easily obtained from routing tables, the ADS system is simple to implement with a small footprint. Using a single ADS, a detection rate of 96% was achieved with no false alarms for attacks in a simulated network[10]. In addition, by using a small number of ADSs at strategic locations in the network, a 100% detection rate was achieved[11].

C. *Non Cryptographic Method of Sinkhole Attack Detection*

Recently, Mobile Agents have been proposed for efficient data dissemination in WSNs [12]. In a typical client/server based WSN, the occurrence of certain events will alert sensors to collect data and send them to a sink node. However, the use of Mobile Agents leads to a new computing paradigm, which is in marked contrast to the traditional client/server-based computing. The Mobile Agent is a special kind of software that propagates over the network either periodically or on demand (when required by the applications). It performs data processing autonomously while migrating from node to node.

Q. Wu [13] presents a genetic algorithm based solution to compute an approximation to the optimal source-visiting sequence. The use of Mobile Agents in computer networks has certain advantages and disadvantages [14], such as code caching, safety and security, depending on the particular scenario. Regardless, they have been successful deployed in many applications ranging from ecommerce to military situation awareness [15]. As described in [12], many inherent advantages (e.g., scalability, extensibility, energy awareness, and reliability) of the Mobile Agent architecture make it more suitable for WSNs than the client/server architecture. In [16], Mobile Agents are found to be particularly useful for data fusion tasks in distributed WSNs.

Early work on routing in dynamic networks using mobile agents by Kramer concentrated on route discovery using agents to continuously track the network topology and update routing tables at all mobile hosts reached. When a route is requested, an agent is sent to discover routes to the destination. These agents analyse the routing tables on the hosts they arrive at and either return a discovered route to the sender or move on to another machine if no route is found. Unfortunately, this method increases network load significantly because mobile agents are constantly moving through the network. Other limitations of Kramer's work are that it is difficult to determine the appropriate number of agents to use and it is not possible to have multiple application specific routing algorithms concurrently in use.

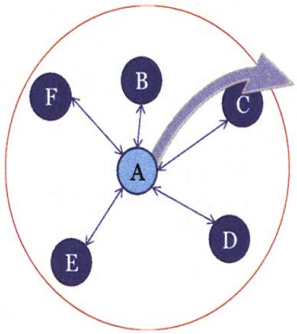
This system schema is designed to make every node aware of the entire network so that a valid node will not listen the cheating information from malicious or compromised node which leads to sinkhole attack. The system uses two algorithms. Agent navigation algorithm tells how does a mobile agent gives network information to nodes and visits every node. Data routing algorithm tells how a node uses the global network information to route data packets. This method has very high overhead if number of nodes are more in WSN. The complexity in storing the information matrix at every node can be decreased in future by using bloom filter technique or some other reduction technique so that it will be a very efficient method.

D. *Sinkhole Attack Detection Mechanism for LQI based Mesh Routing*

This a method that can detect sinkhole attack for safe data transmission in wireless sensor network which uses LQI based routing[17]. The LQI is measured by the strength or quality of a received packet. LQI can be calculated using receiver energy detection, a signal-to-noise ratio estimation, or a combination of these methods. The LQI measurement shall be performed for each received packet. The minimum and maximum LQI values should be associated with the lowest and highest quality compliant signals detectable by the receiver. LQI values in between should be uniformly distributed between these two limits. A higher LQI value indicates a higher quality link. However, link cost inverts this relationship. In other words, a lower link cost indicates higher quality link.

The following assumptions are used in this detection scheme and include, network is consisted of general nodes and few detection nodes, detector nodes have longer-lasting batteries than general sensor nodes, detector nodes can intercommunicate through exclusive channel or other device, detector nodes can act by promiscuous mode and watch all surrounding Routing Request/Reply messages, all sensor nodes have no mobility basically.

Each node calculates LQI value with neighbourhood nodes at Network Initialization Phase. Each node calculates link cost by LQI value that was measured in communication with neighbourhood node and keep smaller value comparing with previous link cost. If this process is repeated enough, each node can make minimum link cost table with neighbourhood nodes. Fig. 2 shows minimum link cost table as an example. Minimum link cost table is used to detect attack when malicious node tries to change the routing path by sending very strong signal artificially.



Neighbor List	Minimum Link cost
B	34
C	78
D	33
E	75
F	50

Fig. 2 Example of Minimum Link Cost Table

Detector nodes perform following process additionally. Detector node searches surrounding detector nodes. And then, they records optimal path cost (accumulated link cost) between each detector node [18]. Usually, LQI based Routing accumulates link cost of each routing path and calculates path cost. Then it selects route that have the smallest cost among them as the optimum path. Therefore, packet transfers following optimal path. Fig. 3 shows an example; path cost of optimal path is 204. But path cost of path that via sinkhole node is 249. Therefore, packet transfers following optimal path.

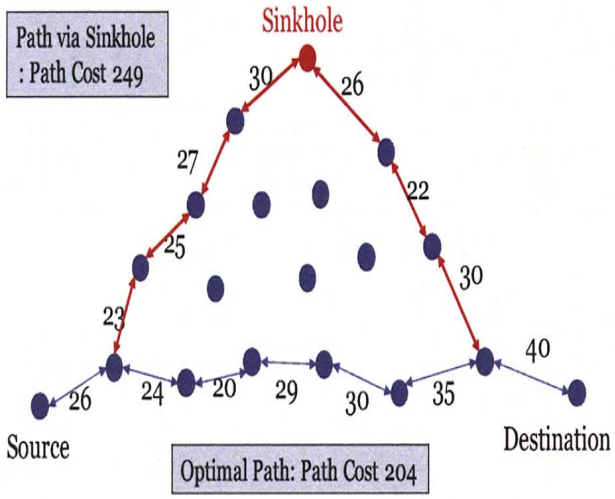


Fig. 3 Path cost between two nodes

In this situation, malicious node accomplishes sinkhole attack as follows:

Method 1: Transmit Routing Request/Reply packet abnormally strong so that neighbourhood nodes may recognize that link quality is very good

Method 2: During Route Discovery phase, changes the LQI to the smallest value.

If malicious node uses these methods, it can perform sinkhole attack successfully. Fig. 4 shows an example, if malicious node uses above method, sinkhole attack can be successful because the modified total path cost is 201. However the original value is 249.

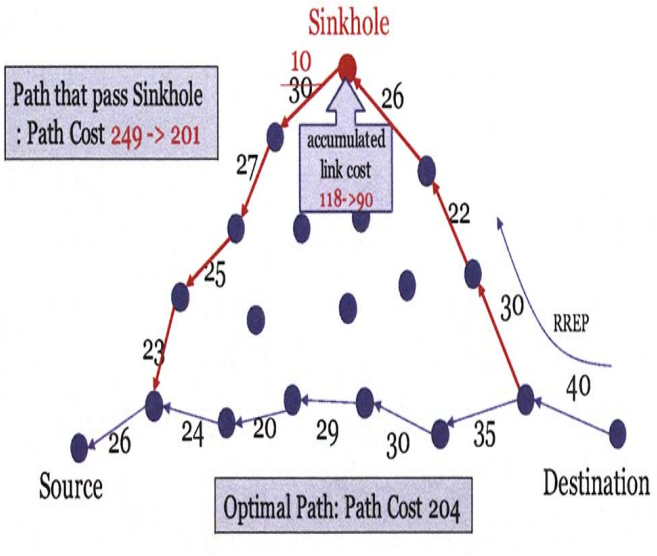


Fig. 4 Path cost when Sinkhole attack is attempted

To detect this attack, two methods are available.

For Method 1: When malicious node forges and sends routing request/reply message, receiving node refers minimum link cost table and examines strength of signal.

$$\textbf{LinkCost}_{cur} < \textbf{LinkCost} * C$$

Here, C means tolerance extent of the received signal. If above condition is found to be true, neighbour node can judge that message is forged.

For Method 2: If malicious node forges accumulated link cost in routing request/reply message, detection is impossible by the above first method. In this case, it can detect attack by using detector node. Detector nodes watch all routing reply messages in its range. In case of sinkhole attack, forged routing reply message is collected by surrounding detector nodes.

Routing Reply Packet is suitable for detection because RREP packets are uni-casted not broadcasted as RREQ.

$$\textbf{Increment of link Cost} < \textbf{PostCost}_{DD} - \textbf{LinkCost}_{DN}$$

- Increment of LinkCost: Increment of accumulated link cost in routing reply message
- PathCost: Minimum path cost between detector nodes
- LinkCost: Link cost between detector node and node that send routing reply message

If the condition in 2 is true, it means that RREP message is transferred to better path than recorded optimum path. As a consequence, its result becomes false. Therefore, detector nodes able to find the sinkhole attack. For instance, in the Fig. 5, detector nodes observe accumulated link cost in RREP message which is transmitted from the neighbour nodes. The detector node I collects RREP message from the node A and the detector node II collects RREP message from the node B.

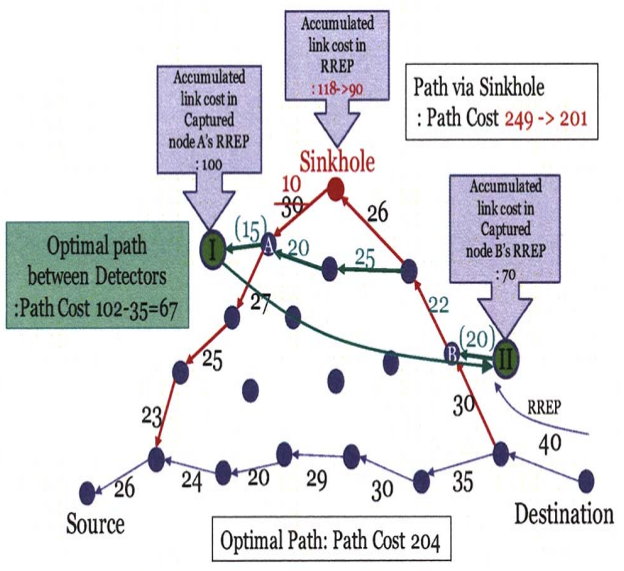


Fig. 5 Example of sinkhole attack detection

The accumulated link cost increment in that observed RREP messages of detector node I and II shows the path cost between node A and B; where the incremented value is 30(100-70=30). On the other hand, in the network initialization phase, calculated minimum path cost between Detector node I and II is 102. And minimum link cost between Detector node I and A is 15. In addition, minimum link cost between Detector node II and B is 20. So minimum path cost between node A and B is 67(102-15-20=67) based on the calculated minimum path cost. As a consequence, if path cost which is calculated between node A and B is smaller than the minimum path cost, it is considered as an attack.

This algorithm consists of network initialization phase and attack detection phase. Network initialization phase collects basic information for detection of sinkhole attack. General nodes collect minimum link cost between each neighbourhood node. Detector nodes compute minimum path cost with surrounding detector nodes as well as link cost with each neighbourhood node. In attack detection phase, we presented two attack detection methods according to the actions of malicious node. We use detector node and detect forgery ofpath cost in routing request message. And we detect abnormally strong signal by referring minimum neighbour link cost table.

V. SUMMARY

Robust security mechanisms are vital to the wide acceptance and use of sensor networks for many applications. Key management in turn is one the most important aspects in any security architecture. Various peculiarities of Wireless Sensor Networks make the development of good key management scheme a challenging task. The diverse nature of WSN usage makes it unreasonable to look for some particular approach that would be suitable for all cases.

REFERENCES

[1] F. Akyildiz and I.H. Kasimoglu, "Wireless Sensor and Actor Networks: Research Challenges,"; Ad Hoc Networks, vol. 2, no. 4, pp. 351-367, Oct. 2004.

[2] Martins, D., Guyennet, H.: Wireless Sensor Network Attacks and Security Mechanisms: A Short Survey. 2010 13th International Conference on Network-Based Information Systems. pp. 313–320. IEEE (2010).

[3] Pandey, A., Tripathi, R.C.: A Survey on Wireless Sensor Networks Security. Int. J. Comput. Appl. IJCA. 3, 43–49 (2010).

[4] Ngai, E.C.H., Liu, J., Lyu, M.R.: An efficient intruder detection algorithm against sinkhole attacks in wireless sensor networks. Comput. Commun. 30, 2353–2364 (2007).

[5] Yanchao Zhang, Wei Liu, Wenjing Lou, Yuguang Fang, "Location-Based Compromise-Tolerant Security Mechanisms for Wireless Sensor Networks", IEEE journal on selected areas in communications, vol. 24, no. 2, February 2006.

[6] A. Cerpa, J. Elson, D. Estrin, L. Girod, M. Hamilton, and J. Zhao, "Habitat monitoring: Application driver for wireless communications technology," in Proc. ACM SIGCOMM Workshop Data Comm. Latin America and the Caribbean, Costa Rica, Apr. 2001, pp. 20–41.

[7] B. Karp and H. Kung, "GPSR: Greedy perimeter stateless routing for wireless networks," in Proc. ACM MobiCom, Boston, MA, Aug. 2000, pp. 243–254.

[8] C. Karlof and D. Wagner, "Secure routing in wireless sensor networks: Attacks and countermeasures," Ad Hoc Netw., vol. 1, no. 2, pp. 293–315, 2003.

[9] J. Newsome, E. Shi, D. Song, and A. Perrig, "The sybil attack in sensor networks: Analysis & defenses," in Proc. 3rd Int. Symp. Inf. Process. Sensor Netw., Berkeley, CA, Apr. 2004, pp. 259–268.

[10] A. Mishra, K. Nadkarni, A. Patcha, "Intrusion detection in wireless adhoc networks," IEEE Wireless Communications, vol. 11(1), pp. 48-60, Feb. 2004.

[11] Daniel Dallas, Christopher Leckie, Kotagiri Ramamohanarao, "Hop-Count Monitoring: Detecting Sinkhole Attacks in Wireless Sensor Networks", 1-4244-1230-7/07/©2007 IEEE.

[12] Hairong Qi, Yingyue Xu, Xiaoling Wang, "Mobile-Agent- Based Collaborative Signal and Information Processing in Sensor Networks," in Proceeding of the IEEE, Vol. 91, NO. 8, pp.1172-1183, Aug. 2003.

[13] Wu, Q., Rao, N.S.V., Barhen, J., etc, "On computing mobile agent routes for data fusion in distributed sensor networks," IEEE Transactions on Knowledge and Data Engineering, Vol.16 , NO. 6, pp. 740-753, June 2004.

[14] S. Capkun, L. Buttyan, J. Hubaux, SECTOR: Secure Traking of Node Encounters in Multi-hop Wireless Networks, in: proc. Of SASN 2003. Fairfax, Virginia, October 2003.

[15] K.N. Ross and R.D. Chaney, "Mobile Agents in Adaptive Hierarchical Bayesian Networks for Global Awareness," Proc. IEEE Int'l Conf. Systems, Man, and Cybernetics, pp. 2207-2212, 1998.

[16] Hairong Qi, Iyengar, S., Chakrabarty, K., "Multiresolution data integration using mobile agents in distributed sensor networks," IEEE Transactions on Systems, Man and Cybernetics, Vol.31, No.3 , pp. 383-391, Aug. 2001

[17] 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", RFC 3561, July 2003.

[18] Ji-Hoon Yun, Il-Hwan Kim, Jae-Han Lim, and Seung-Woo Seo, "WODEM: Wormhole Attack Defense Mechanism in Wireless Sensor Networks", ICUCT 2006, LNCS 4412, pp. 200-209, 2007.