# Securing on Demand Source Routing Protocol in Mobile Ad-Hoc Networks by Wormhole Attacks

**Palash Butle[1], Renuka Dev[2], Ankita Dalvi[3], Manisha Dautpure[4]**

[1,2,3,4] *Computer science and Engineering SGBAU Amravati (India)*

---

**Abstract -** *A mobile ad hoc network (MANET), is a kind of wireless network which is infrastructure-less and adaptive in nature .MANET follows multicast communication as many applications in MANET are group oriented in nature. MANET is susceptible to different types of attack due to their unique and inherent characteristics such as lack of centralized authority, limited node's battery power etc. One of the most powerful attacks in Ad-hoc networks is the wormhole attack. Vampire attack is the type of resource depletion attack in which a malicious node is generated and these malicious nodes creates and send messages with more enjoyment of node's battery power than with the honest node and leads to slow depletion of node's battery life. In this paper we proposed different mitigation method to detect and to reduce vampire attack .We considered the effect of vampire attack on AODV protocol and the theoretical based simulated graphs are also presented to analyze the performance of the Ad-Hoc network in the presence and absence of Vampire attack by using network simulator 2(ns2).*

***Key Words*: Denial of service, security, routing, ad-hoc networks, draining life.**

## 1. INTRODUCTION

Wireless networking devices uses some sort of radio frequencies in air to transmit and receive data instead of using any physical media. Wireless networking devices operates in two mode i.e. infrastructure mode and ad-hoc mode. In infrastructure mode a connection is establish between wireless network and a wired Ethernet network and for the infrastructure mode there is requirement of at least one base station or access point. While the Ad-hoc mode in contrast to the infrastructure mode there is no requirement of any access point. Ad-hoc mode is a method of wireless devices to directly communicate with each other. Mobile Ad-Hoc network do not posses any permanent infrastructure or physical backbone. Mobile nodes in the network dynamically setup paths among themselves to transmit packets to the destination. Due to Mobility of the nodes MANET should have some characteristics which make them distinguishable from conventional wired networks. MANET are self organizing and adaptive in nature which means that the nodes are spontaneously forming and deforming the networks and updating the routing table associated to each node. Thus MANET follows dynamic routing protocol.

### 1.1 Routing protocol

Routing is the process of moving a packet of data from source to destination. Routing is a key feature of internetworking. Each intermediary computer performs routing by passing along the message to the next computer. Part of this process involves analyzing a routing table to determine the best path. Routing protocol may be static routing protocol or dynamic routing protocol.

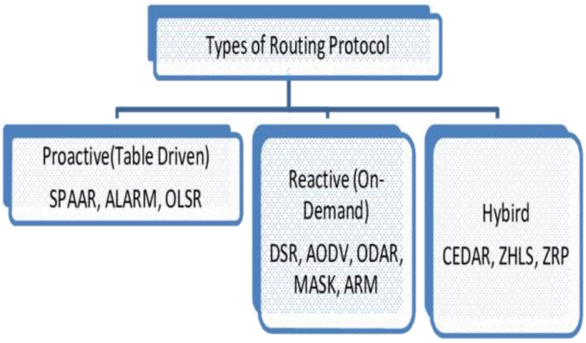


**Fig -1**: Routing Protocol

There are mainly two routing protocols i.e. proactive and reactive. Table driven routing protocols which is also called as proactive protocol since they maintain the routing information even before it is needed. Proactive protocol classified into four types FSR, FSLS, OLSR, and TBRPF. The proactive protocols are not suitable for larger networks, as they need to maintain node entries for each and every node in the routing table of every node. On demand routing protocol are also called as since they don't maintain routing information or routing activity at the network nodes if there is no communication. If a node wants to send a packet to another node then this protocol searches for the route in an on-demand manner and establishes in order to transmit and receive the packets. Reactive routing protocol is of two types AODV and DSR. Hybrid Routing, commonly referred to as balanced-hybrid routing, is a combination of distance-vector routing, which works by sharing its knowledge of the entire network with its neighbors and link-state routing which works by having the routers tell every router on the network about its closest neighbors. In this paper we are considering the affect of wormhole attack on MANET. We propose a clustering method to mitigate the affect of Wormhole attack. And we are using the Ad-Hoc On Demand Distant Vector Routing (AODV) protocol to secure the network. In MANET communication starts between the nodes within each other's transmission range by broadcasting control messages between themselves directly. However, nodes beyond each other's range have to rely on some other node to relay messages. Challenges of MANET lead to security issues which include routing security, data forwarding security, link layer security, key management, intrusion detection and so on. In MANET many applications are group oriented in nature and can therefore benefit from multicast communication. Due to these inherent characteristics of MANET they are susceptible to different security attacks.

### 1.2 Security attack in MANET

The security attacks in MANET can be categorized on the basis of the source of the attacks i.e. Internal or External, and on the behavior of the attack i.e. Passive or Active attack. The classification of security attack is intrinsic because the attacker can feat either of the attack.

**Passive attack:** In passive attack attacker does not disturb the usual operation of the network, it just snoops the data exchanged in the network without altering it.

**Active Attack:** In contrast to passive attack an active attack goes to alter or destroy the data being exchanged in the network. Means in general passive attack take the data without altering it active attack disturb and alter the data. According to domain of the attacks, the attacks can be classified into two categories: Insider and Outsider attacks. Insider attacks are done by compromised nodes, which are actually the part of MANET network. Outsider attacks are carried out by outside or external nodes. Outsider attacks are easy to recognize and can be detected/prevented with cryptographic techniques (Encryption, Decryption, Private Key. However, insider attacks are very complicated. These attacks cannot be prevented with simple cryptographic techniques

## 2 Related Works:

Mirjeta Alinci et al. [3] have reviewed several clustering algorithms which help us to organize mobile ad hoc networks in a hierarchical manner and presented their main characteristics. Most of the clustering schemes are based on important issues such as stability of cluster, maximizing the network lifetime, the energy consumption of mobile nodes and maintenance. From all the revealed schemes combined-metrics based clustering scheme is better because it provides high stability in cluster and creates less number of clusters. Daniel J. Bernstein et al. [7] gives an overall understanding of TCP and SYN cookies. There are several disparate ideas woven together on the TCP and SYN cookies threads. Even though most TCP implementations have a common ancestor, the details depend on the operating system and even the version of the operating system. Therefore any attempt at a general discussion will need to make some assumptions for the sake of being definite and the conclusions may not apply to all implementations or even in precise detail to any current implementation.

Martin Feldhofer et al. [19] have explained a security-enhanced RFID system which allows the strong cryptographic authentication. With these security-enhanced RFID systems, we pave the way for new security-demanding applications and for the everyday usage of RFID technology. A symmetric challenge-response authentication protocol was proposed which was integrated into the existing ISO/IEC 18000 standard. The AES implementation has a chip area of 3,595 gates and has a current consumption of 8.15 μA at a frequency of 100 kHz. The encryption of 128 bits requires about 1000 clock cycles.

Yurong Xu et al. [18] explained the wormhole geographic distributed detection (WGDD) algorithm that employs a hop counting technique as a probe procedure for wormholes, reconstructs local maps using multidimensional scaling at each node, and uses a novel "diameter" feature to detect distortions produced by wormholes. Unlike other wormhole detection algorithms, it does not require anchor nodes, additional hardware (e.g., directional antennas and accurate clocks) or the manual setup of networks. Even so, it can rapidly provide the locations of wormholes, which is useful for implementing countermeasures. Because the algorithm is distributed, each node can potentially detect the distortions produced by a wormhole, which increases the likelihood of wormhole detection.

Majid Khabbazian et al. [2] proposed a method to study the effect of the wormhole attack in shortest path routing protocols. Using analytical and simulation results, we showed that two strategically located attackers can on average disrupt 32% of all communications across the network. We also considered the effect of the wormhole attack launched by n ¸ 2 malicious nodes and showed that on average at least 1/n of all communications are not affected by the attack. Finally, we proposed a robust and secure on demand distance vector routing protocol to counter the wormhole attack launched in the hidden or participation mode.

Mohammad Rezaee et al. [9] gives a detail view of new clustering protocol for MANET. The proposed protocol uses a clustering protocol which attempts to create stable clusters quickly. In the proposed protocol, due to the weight group, the cluster creation is done very quickly which causes the network services to be more accessible. Recreating of clusters is rarely executed, and when two clusters locate in the same range, one of them becomes the gateway of other node. This causes to prevent the creation of most constructions. Nodes which are not members of a cluster, in the case of having GATEWAY nodes in their neighborhoods, can use them for purpose of their executing service (e.g. routing). In the proposed protocol the routing is also done quickly.

## 3 AODV Working:

An Ad Hoc On-Demand Distance Vector (AODV) is a routing protocol designed for wireless and mobile ad hoc networks. This protocol establishes routes to destinations on demand and supports both unicast and multicast routing. The AODV protocol was jointly developed by Nokia Research Center, the University of California, Santa Barbara and the University of Cincinnati in 1991.The AODV protocol builds routes between nodes only if they are requested by source nodes. AODV is therefore considered an on-demand algorithm and does not create any extra traffic for communication along links. AODV makes use of sequence numbers to ensure route freshness. They are self-starting and loop-free besides scaling to numerous mobile nodes. In AODV, networks are silent until connections are established. Network nodes that need connections broadcast a request for connection. The remaining AODV nodes forward the message and record the node that requested a connection. Thus, they create a series of temporary routes back to the requesting node.

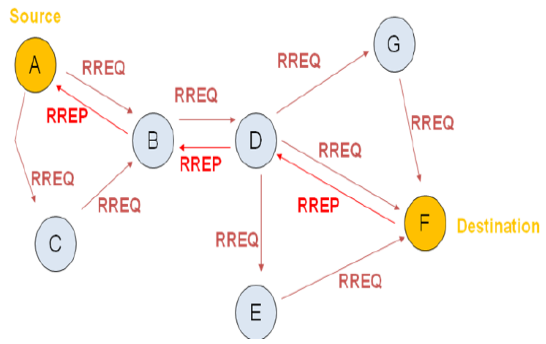


**Fig -2**: AODV Working

A node that receives such messages and holds a route to a desired node sends a backward message through temporary routes to the requesting node. The node that initiated the request uses the route containing the least number of hops through other nodes. The entries that are not used in routing tables are recycled after some time. If a link fails, the routing error is passed back to the transmitting node and the process is repeated.

## 4 Wormhole Attack:

The assaulting hub catches the parcels from one area and transmits them to other far off found hub which disperses them locally. A wormhole assault can undoubtedly be propelled by the assailant without knowing about the system or trading off any real hubs or cryptographic instruments. Wormhole attack is of two types Hidden attack and Exposed attack.

**Hidden attack-** genuine routers involved in the data transmission are unaware of the presence of malicious nodes in the path.

**Exposed Attack-** In exposed attack, existence of the malicious nodes is known to the genuine routers but their malicious behavior is not known.

### 4.1 How it is launched:

In hidden attack case, attackers do not include their ID during the transmission of route request packet (RREQ). Hence source and destination consider themselves as direct neighbor to each other. In exposed attack case, both attackers are located in multi-hop. During RREQ transmission second attackers modify the hop count field in RREQ packet to least value and pretend like both are direct neighbors so that data transmission can be initiated through them.

### 4.2 How it degrades the network performance:

Wormhole attacker either can drop the data or redirect the data to other nodes in the network. Hence it affects the packet delivery ratio and throughput in the network. In some cases, if the wormhole attackers deliver the data to destination it will be reached with certain delay due to the creation long path by wormhole attackers.

### 4.3 How to create wormhole attack in NS2:

Mobile Ad-hoc network is created with the number of nodes as run time argument. Each node is configured with wireless node configuration options. Suppose Node 0 is source and Node 1 is destination. Node2 and 3 are wormhole attackers and they are configured to be located far away from each other and Exposed attack is launched here. Routing agent corresponding to the attacker nodes is configured as wormhole1 and wormhole2. AODV routing protocol is used at the network layer. Regarding c++ part, aodv.cc file is modified in such a way that during route discovery process, attacker decreases the hop-count value in RREQ packet and also when the data is transmitted via attacker1 forwards it to attacker2 which drops the data without forwarding to next hop or destination. In MANET mobile nodes have restricted geographical range and sending message to the node that is not in transmission range can be sent through broadcast mechanism. The broadcast mechanism is used by the router for delivery the message to destinations that is not in the sender's range. The router uses routing protocols for accomplishing the broadcast mechanism. The main goal of these protocols was to route the packet efficiently, due to which these routing protocols lacks the security measures. There are various security threats to MANET that can create harm to our network like black hole, gray hole, eavesdropping and wormhole attack. Security in mobile ad-hoc network is the current important issue of network. The Services of network like confidentiality and integrity of data is attained by facing and solving the security issue of MANET. The dynamic topology and open nature makes the wireless network (especially Mobile Ad-hoc network) more vulnerable to security threats.

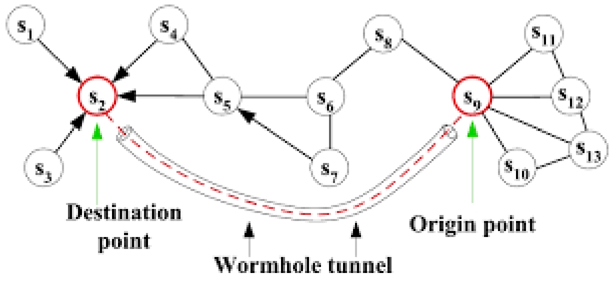


**Fig-3:** Wormhole attack

### 4.4 Impacts of wormhole attack

Sudden Decreases in Hops: When the wormhole assault is eaten and makes the connection and pulls in the bundles to exchange so it reason for decline in jumps because of utilization long separation channel as opposed to utilizing many bounces.

Sudden Increase in Path Delays: Some of the ways may not take after the publicized false-interface, yet they may utilize a few hubs required in the wormhole assault. Longer Propagation Delays: MANET is powerless against noxious assaults because of the high piece blunder rates, longer engendering deferrals, and low transfer speed, when the bundle needs to transmit by wormhole, it might get the parcel and on account of postponement to transmit the bundle Diminish in Network Utilization: when the bundles are exchange through the wormhole connect it reason for lessening system use because of utilization wormhole burrow as transmission channel and alternate courses are free.

### 4.5 Countermeasures

We are dealing with the wormhole attack which is energy depletion attack i.e. it consumes more energy of the nodes while sending the packets or transmitting the data. To deal with this attack in network we need a system which can detect, identify and remove the attack. As we are dealing with the vampire attack which is either sending packets through long route or sending the packets through the nodes which involves the loop in the sending path of the network that means the vampire attack is initially attacking the nodes and then through these nodes attack starts to operate maliciously on packet. So there is need to stare at nodes initially to stop the vampire attack from introducing in the network. So in this report we have introduced the new concept called the clustering. To overcome this attack through concept clustering, we will be making the group of the nodes called as the cluster. Each cluster contains group of approximately 20-30 nodes in it. In addition we allocate one node as the master node among the cluster which is called as the head of the cluster. The header node is selected on the basis of the criteria of how old the node is in the clustering or we can say that the oldest node among them all is selected as the header node in the cluster. The header node has most crucial work to do as it is now responsible to manage the network, the header node has all the information of other nodes in the cluster, such as the routing path, the source from which packet is being delivered, the destination to which the packet is to be sent, the information of previous node and also the foremost node. The header node pays attention to every action of node in the cluster i.e. it makes sure that the packet which is to be sent is going through the right path. If somewhere down the line, any misbehave by node exists or certain malicious behaviour by any node in the cluster is noticed the header node instantly takes action against these nodes by suspending them or by isolating them from the communication path. There can be number of clustering units in the field which completely depends upon the number of nodes in the communication.

## 5 RESULTS AND IMPLEMENTATION

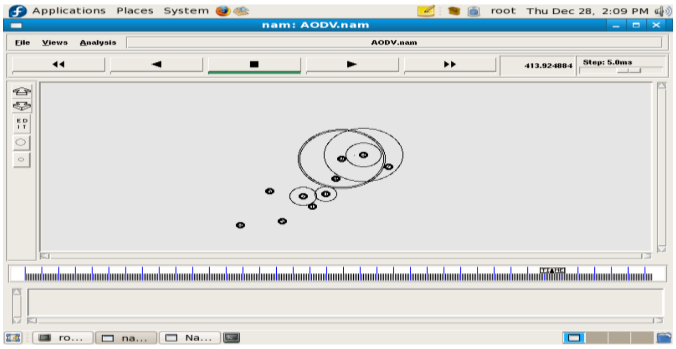
In the implementation we have performed execution of three programs first program is normal routing of Ad-hoc networks .Then next program is Ad-hoc networks with Attack and in the mitigation last program with secure AODV is executed. Clustering is a process that divides the network into interconnected substructures, called clusters. We considered the effect of vampire attack on AODV protocol and the theoretical based simulated graphs are also presented to analyze the performance of the Ad-Hoc network in the presence and absence of Vampire attack by using network simulator 2(ns2).

**Gawk -f filename.awk filename.tr**

Packet delivery ratio is the ratio of packets that are successfully delivered to a destination compared to the number of packets that have been sent by sender. In order to calculate packet delivery ratio we need total number of packets sent and number of received packets.

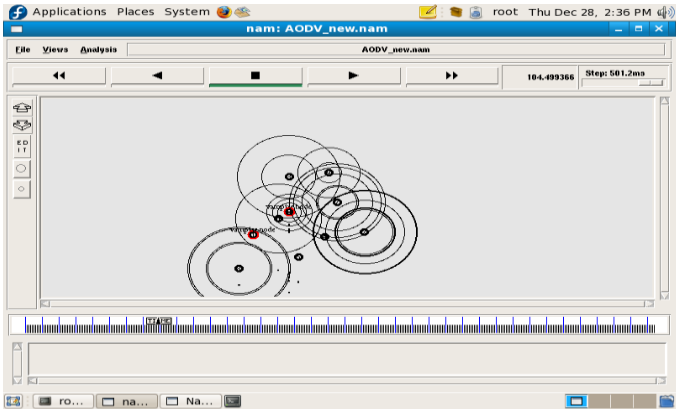
### 5.1 Screenshots

The below screenshot shows the behavior of nodes while performing the transmission of packets in Ad-hoc network. This is the normal scenario without introducing any attack in the network i.e. this is the ideal case.

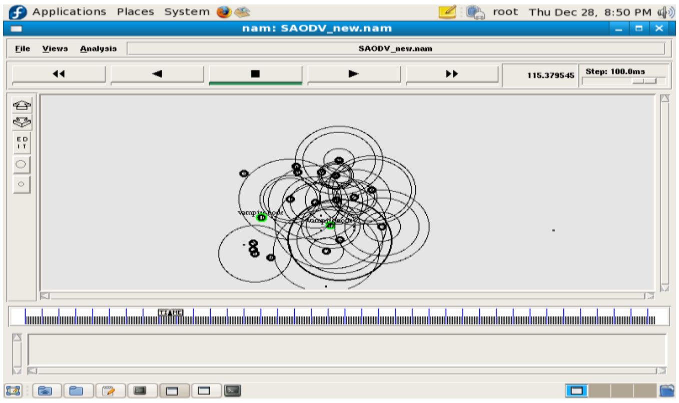


**Snapshot 1:** Normal Scenario of AODV in MANET

The below screenshot shows the malicious activity of the node which is effected by the vampire attack. These particular nodes change the path of the packet which is to be sent and transfers the packet through the unwanted and bulky path.



**Snapshot 2: Attack In MANET**



**Snapshot 3:** Secure AODV

The above screenshot shows the countermeasures applied for the mitigation of vampire attack. The green spotted nodes are the nodes which were previously affected by the vampire attack and now they are cured.

## 5.2 Graphs

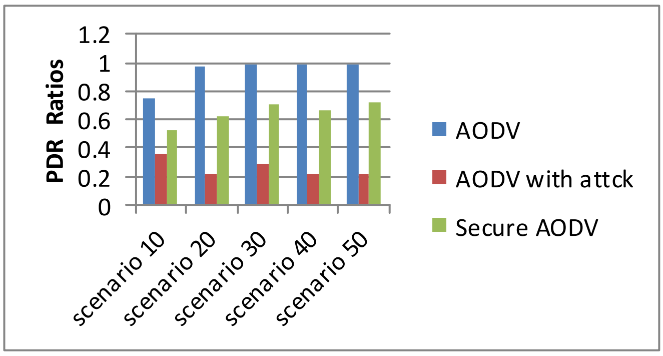


**Fig 4:** PDR Ratios

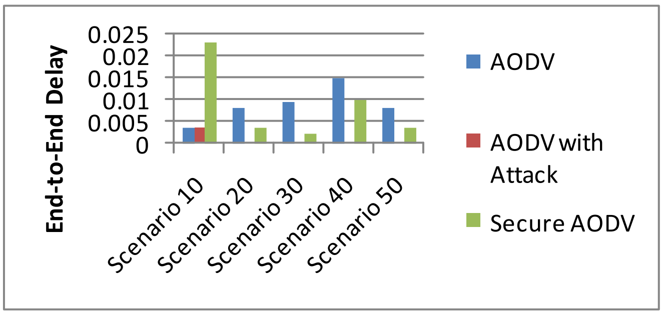


**Fig 5:** End-to-End Delay

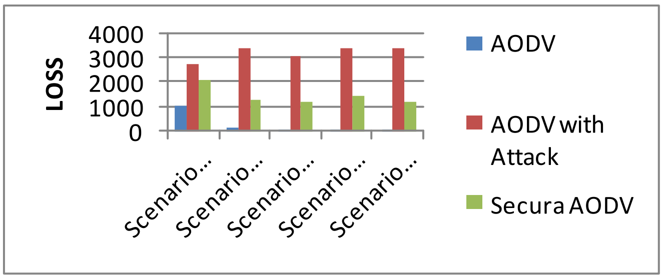


**Fig 6:** Packet Loss

## 6 Conclusion and future scope

In the conclusion we define the vampire attack that the type of resource depletion attack as one of the most powerful attack in mobile ad-hoc network which completely destroy the network by draining battery power from mobile nodes. We proposed different types of vampire attacks such as carousel attack, stretch attack, packet forwarding and directional antenna attack. We explore different mitigation methods to bind the damage from vampire attack. Ad-hoc wireless sensor network promises exciting new applications future work.

## 7 References

[1] Daniel Bernstein and Peter Schwabe, New AES software speed records, INDOCRYPT, 2008.

[2] Majid Khabbazian, Hugues Mercier and Vijay K.Bhargava Wormhole Attack in Wireless Ad Hoc Networks: Analysis and Countermeasure Department of Electrical and Computer Engineering University of British Columbia 2356 Main Mall, Vancouver, BC, Canada V6T 1Z4

[3] Mirjeta Alinci, Evjola Spaho, Algenti Lala and Vladi Kolici , Clustering Algorithms in MANETs: A review 2015 Ninth International Conference on Complex, Intelligent, and Software Intensive Systems

[4] Tuomas Aura, Dos-resistant authentication with client puzzles, International workshop on security protocols, 2001.

[5] Daniel Bernstein and Peter Schwabe, New AES software speed records, INDOCRYPT, 2008.

[6] INSENS: Intrusion-tolerant routing for wireless sensor networks, Computer Communications 29 (2006), no. 2.

[7]Daniel J. Bernstein, Syn cookies, 1996. http://cr.yp.to/syscookies.html

[8]I.F. Blake, G. Seroussi, and N.P. Smart, Elliptic curves in cryptography, Vol. 265, Cambridge University Press, 1999.

[9] Mohammad Rezaee, Mohammad Hossien Yaghmaee A New Clustering Protocol For Mobile Ad-hoc Networks, 2008 Internatioal Symposium on Telecommunications

[10]Haowen Chan and Adrian Perrig, Security and privacy in sensor networks, Computer 36 (2003), no. 10.

[11] Thomas H. Clausen and Philippe Jacquet, Optimized link state routing protocol (OLSR), 2003.

[12]INSENS: Intrusion-tolerant routing for wireless sensor networks, Computer Communications 29 (2006), no. 2.

[13]Packet leashes: A defense against wormhole attacks in wireless Ad-Hoc networks, INFOCOM, 2013.

[14]Jing Deng, Richard Han, and Shivakant Mishra, "Defending against path based DOS attacks in wireless sensor networks" ACM workshop on security of ad hoc and sensor networks, (2005).

[15]Rahul C. Shah and Jan M.Rabaey,"Energy aware routing for low energy ad hoc sensor networks"(2002).

[16]T. English, M. Keller, Ka Lok Man, E. Popovici, M. Schellekens, and W. Marnane, A low-power pairing-based cryptographic accelerator for embedded security applications, SOCC, 2009.

[17]Laura M. Feeney, An energy consumption model for performance analysis of routing protocols for mobile ad hoc networks, Mobile Networks and Applications 6 (2001), no. 3.

[18]Yurong Xu, Guanling Chen, James Ford and Fillia Makedon, DETECTING WORMHOLE ATTACKS IN WIRELESS SENSOR NETWORKS

[19] Martin Feldhofer, Sandra Dominikus, and Johannes Wolkerstorfer, Strong authentication for RFID systems using the AES algorithm, CHES, 2004.