IMPACT OF WORMHOLE ATTACK IN WIRELESS SENSOR NETWORK

Onkar Adarkar[1], Rupesh Mane[2], Prof. Dipali Shah

[1,2]STUDENT OF DEPT OF MCA NCRD'S SIMS STUDIES, NERUL.MAHARASHTRA, INDIA
[3]ASSOCIATE PROFESSOR, DEPT OF MCA NCRD'S SIMS STUDIES, NERUL.MAHARASHTRA, INDIA.

Abstract – *Lots of different attacks like Wormhole attack in the wireless sensor network is one of the growing research areas in a few years. Tiny devices are known as Wireless Sensor Network [WSN] which have limited energy, computational power, transmission range, and memory. Wireless sensor networks are available in the open and unsecured environment. We propose the wormhole attack, a severe attack in ad hoc networks that is particularly challenging to defend against. The wormhole attack is possible even if the attacker has not compromised any hosts, and even if all communication provides authenticity and confidentiality. In wormhole attacks, which undermines the performance gain of network coding. A wireless sensor network (WSN) consists of a large number of sensor nodes with limited batteries, the sensor devices are deployed randomly on a zone to collect data. This paper is focused on impact of wormhole detection and prevention with different types of recovery method.*

***Key Words*: Wireless sensor network, Security, Attacks, Challenges, Wormhole, packet Leash, Ad hoc Network.**

1.INTRODUCTION

The promise [1] of mobile ad hoc networks to solve challenging real-world problems continues to attract attention from industrial and academic research projects. Applications that may require secure communications include emergency response operations, military or police networks, and safety-critical business operations such as oil drilling platforms or mining operations. For example in an emergency, response operations such as after a natural disaster like a flood, tornado, and hurricane, or earthquake, ad hoc networks could be used for real-time safety feedback; regular communication Networks may be damaged, so emergency rescue teams might rely upon ad hoc networks for communication.

In this paper, we research on different types of attacks and its challenges to get protection from wormhole attack, and we present a new, general mechanism for detecting and thus defending against wormhole attacks. In this attack, an attacker store records into a packet, or individual bits from a packet, at one location in the network, tunnels the packet (possibly selectively) to another location and replays it there. We discuss the procedure of packet leashes to detect wormhole attacks, and we present two types of leashes: geographic leashes and temporal leashes. We design an efficient authentication protocol, called TIK, for use with temporal leashes.

II. PROBLEM STATEMENT

In a wormhole attack, an attacker receives packets in bits at one location in the whole network, "tunnels" them to another location in the network and then repeats them into the network from that location. For tunnel spacing longer than the normal wireless transmission range of a single hop network. It is possible for an attacker to move each bit of packets directly to the wormhole, without waiting for the entire packet to be received before beginning the tunnel. This attack hence prevents any programs other than throughout the wormhole from being found, and if the attacker is near the initiator of the Route Discovery, this assault can even prevent programs more than two hops long from being seen. Permissible modes for the attacker to then misuse the wormhole include dropping rather than transmitting all data packets, thereby creating a strong Denial-of-Service attack (not another route to the destination can be identified as long as the attacker maintains the wormhole for ROUTE REQUEST Packets), or selectively discarding or modifying certain data packets. The neighbor discovery mechanisms of periodic (proactive) routing network protocols such as DSDV [7], OLSR [9] rely heavily on the reception of broadcast packets as a means for neighbor detection and are also extremely fenceless to this attack. In such systems, an attacker could relay the authentication exchanges to gain unauthorized access.

WSN Threats And Recovery Methods

We can examine wormhole attack as a two-phase method started by one or several malicious nodes. The various threats prompt by the wormhole attack are selective dropping or modification of data packets, switching off the wormhole link periodically in order to Good node Malicious generates unnecessary routing activities, they also try to disrupt the data flow. It is also possible for the attacker to simply record the traffic for later analysis.

This section summarizes the related works in the literature for wormhole attack detection &Prevention as shown in the table 1 below.

Sr. No.	Wormhole recovery methods		
	Method	Requirement	Commentary
1	Packet leashes, geographical	GPS coordinates of Every node; Loosely synchronizedclocks (ms)	Robust, straightforward solution; inherits general limitations of GPS technology
2	Packet leashes, temporal	Tightly synchronized clocks (ns)	**Impractical;** required time synchronization level not currently achievable in to sensor networks
3	Packet leashes, end-to-end	GPS coordinates; Loosely synchronized clocks (ms)	Inherits limitations of GPS technology
4	Time of flight	Hardware enabling one-bit message and immediate replies without CPU involvement	**Impractical;** likely to require MAC-layer modifications
5	Directional Antennas	Directional antennas on all nodes or several nodes with both GPS and directional antennas	Good solutions for networks relying on directional antennas, but not directly applicable to other networks
6	Network visualization Not readily applicable to mobile networks.	Centralized controller	Seems promising; Works best on dense networks; Mobility not studied; Varied terrains not studied
7	Localization	Location-aware 'guard' Nodes	Good solution for sensor networks
8	LiteWorp	none	Applicable only to static stationary networks; **Impractical**
9	Statistical analysis	no requirements	Works only with multi-path on demand protocols;
10.	MGM	Light weight local monitoring	For necessary condition, the heavy weight RV protocol is triggered. it is more resource efficient and powerful

Table 1.Summary of various defenses mechanisms for Wormhole attack

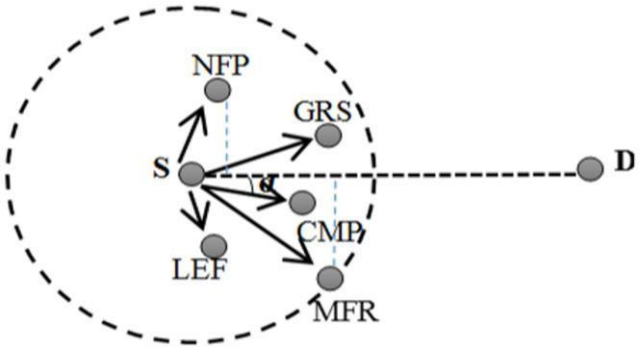
III. DETECTING WORMHOLEATTACKS

In this part, we introduce the concept of a packet leash as a general mechanism for detecting and protecting against wormhole attacks. A leash is an information that is added in a packet structured to ban the packet's most allowed to the transmission distance. Leashes are structured to protect against wormholes across a separate wireless transmission;when we packet broadcasted over multiple hops, then every transmission expected the use of the new leash.

A. Geographical Leashes

each node must know its location and all nodes must have loosely synchronized clocks. Location-based routing protocols are an important group of protocols in WSNs in which position information is used to route data towards the desired regions (sinkhole). Location-based routing is also known as position-based, directional, geographic, or geometric routing [15]. This section briefly reviews the geographic routing protocols.

The geographic routing protocols are classified into five groups, based on how the next hop is chosen. The Greedy Routing Scheme (GRS) is the first group of a geographic routing protocol in which each node selects the best node among the neighbors that is closest to the destination. GPSR is an example algorithm falls in this category in which a packet should be forwarded hop by hop based on GRS and available local information, which is actually gathered by the Global Positioning System (GPS) until it meets a void area. In this way, the received message must be passed to the first neighbor counterclockwise about itself [16]. The next group of the geographic routing protocols is called Most-Forward-within-R strategy (MFR). In MFR, the packet is sent to the most forward node to destination among the neighbors of the sender based on the transmission range (R). The third approach is the Nearest-Forward-Progress scheme (NFP) in which the nearest neighbor to the transmitter is chosen to send data. The compass routing scheme (CMP) is the fourth system among the geographical routing protocols. In this scheme, the neighbor that has a minimum angle to the imaginary line between the source and destination is selected as the next hop. Low-energy forward scheme (LEF) selects a neighbor that requires a minimum energy to transmit packets. However, among these geographic routing protocols, the GRS is more popular and more applicable than the other methods due to the rate of delay and energy of this method [17, 18]. Fig. 1 illustrates how the next node will be selected in the different type of forwarding approaches to transfer the packet from source (S) to destination (D) node.

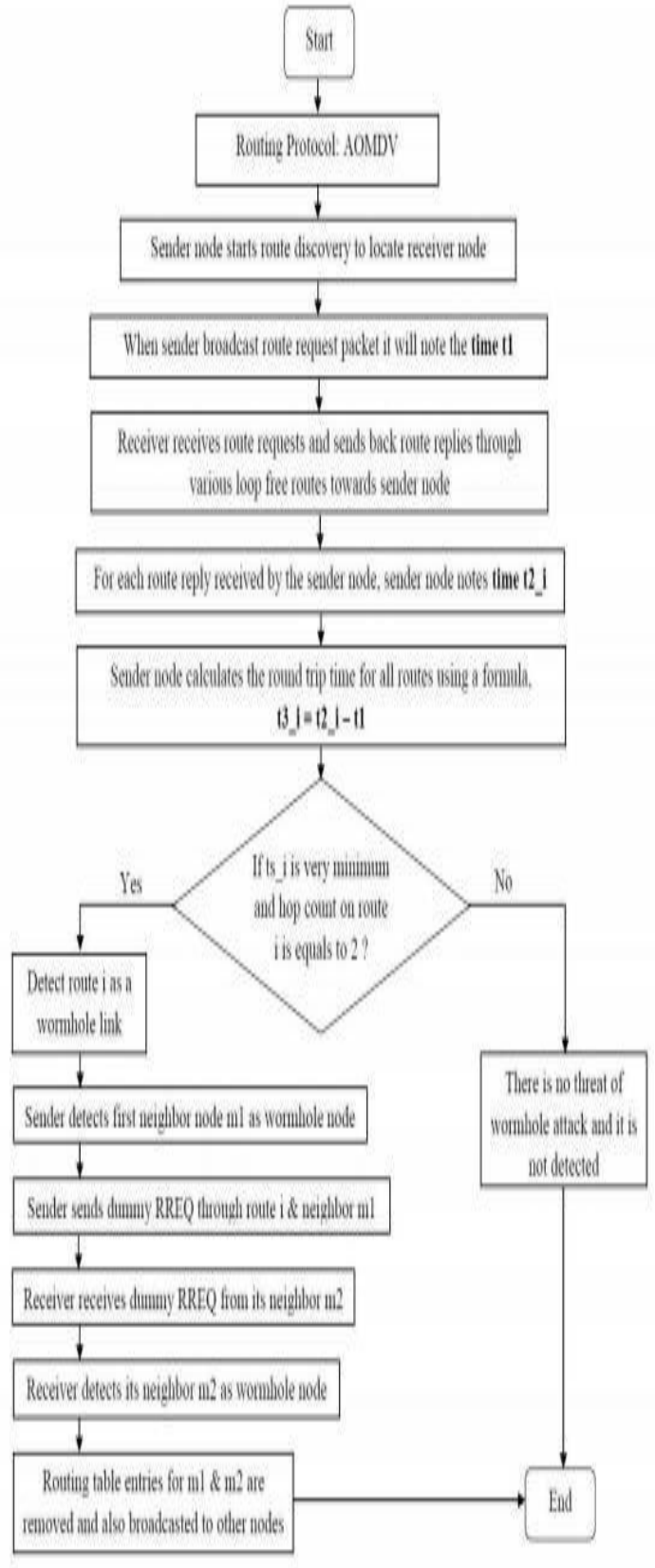


B. Temporal Leashes

To build a temporal leash, in general, all nodes must have tightly synchronized clocks, such that most of the difference between any two nodes' clocks is! The value of the parameter! Must be known by all nodes in the network, and for temporal leashes, generally must be on the order of a few microseconds or even hundreds of nanoseconds. This level of time synchronization can be accomplished now with off- the-shelf hardware based on LORAN-C [5], WWVB [6], GPS [3], [13], or on-chip atomic clocks currently under development at NIST [4]; although such hardware is not currently a common part of wireless network nodes, it can be deployed in networks today and is expected to become more widely utilized in future systems at reduced expense, size, weight, and power consumption.Alternatively, a temporal leash is invented by alternatively including termination time in the packet, after which the receiver does not receive the packet; based on the allowed highest transmission distance and the speed of light, the sender initiates this expiration time in the packet as an offset from the time at which it forwards the packet.

The Proposed mechanism to detectand prevent wormhole attack

To discover multiple paths between the source and the destination in every route discovery Ad-hoc On-demand Multipath Distance Vector routing protocol (AOMDV) is used which is an extension of the AODV protocol.
Whenever the destination receives the RREQ packet it sends RREP packet to the source along the same path through which the RREQ packet has arrived. For all RREQ packets arrived through other routes the RREP packets are sent along the same path. All the paths are stored in the routing table at the source node. The main concept in AOMDV is during route discovery procedure to estimate multiple paths for contending link failure. When AOMDV builds multiple paths, it will select the main path for data transmission which is based on the time of routing establishment. Only when the main path is down other paths can be effective and the earliest one will be regardedthe best one.[19]



VI. EVALUATION

A. TIK Performance

To evaluate the suitability of our function in ad hoc networks for use, we studied computational power and memory which are currently receivable in all type of mobile devices. To scale the number of repeated hashes that can be counted per second, we improved the MD5 hash code from ISI [12] to achieve supreme performance for repeated hashing.

B. Security Analysis

A malicious sender requests false timestamp or location that deliver a legitimate receiver to have incorrect beliefs about whether or packet does not tunnel. When geographic leashes are used in conjunction with digital signatures, nodes may be able to detect a malicious node and spread that information to another node, as discussed in Section IV-C.

Comparison Between Geographic and Temporal Leashes

Geographical Leashes	
pros	cons
can be used in conjunction with radio propagation model, allowing them to detect tunnels through obstacles	require more general broadcast authentication mechanism increasing computation, overhead
do not require tight time synchronization	location info increases overhead
can be used until maximum range is $< 2v\Delta$ (v is the max movement speed of any node)	

Temporal Leashes	
pros	cons
highly efficient, especially when used with TIK	tight time synchronization
	can not be used if max range $< c\ \Delta$ (c is the speed of light, Δ is max clock sync error)

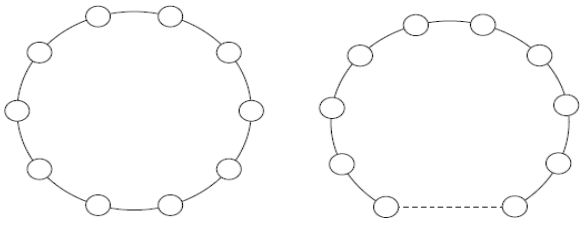


Fig.3. These two network topologies are not distinguishable by topology based wormhole detection, yet one contains a wormhole and the other does not. The dotted line in the figure on the left represents the wormhole.

D. Security of Topology-Based Approaches

Some researchers [14], have created a method to detect wormholes by constructing a model of the network topology based on identify incorrect distance measurements between neighbor nodes that can receive packets from each other (possibly through a wormhole); wormholes can then be visualized in this topology by the anomalies they introduce, bending the topology so that the nodes on either side of the wormhole appear closer together. However, such topology- based approaches alone cannot detect all wormholes.

Contribution

In the beginning, we focus on the impact of wormhole attack in wireless networks. Then present a very detailed discussion about different types of existing solutions against wormhole attacks along with the effects of long transmission on these solutions. Study different papers on wormhole attack and their recovery methods which is mention in this paper. We study packet leashes which have two types 1) Geographical Leashes, 2) Temporal Leashes. Then compare both each other. Also we found how to prevent this types of attacks using TIK. It is an third party and dangerous attack which are very dangerous.
This comparison gives the complete overview of each type of solution against wormhole attacks including their network type, routing protocol, hardware or clock synchronization requirements, type of wormhole detected and consideration of multi-rate transmission.

CONCLUSIONS

In this paper, we have introduced the *wormhole attack*, a powerful attack that can have serious consequences on many proposed ad hoc network routing protocols; the wormhole attack may also be exploited in other types of networks and applications, such as wireless access control systems based on physical proximity. To detect and defend against the
wormhole attack, we introduced *packet leashes*, which may be either *geographic* or *temporal* leashes, to restrict the maximum transmission distance of a packet. Finally, to implement temporal leashes, we presented the design and performance analysis of a novel, efficient protocol, called TIK, which also provides instant authentication of received packets.
When we use conjunction with well-defined timestamps and tight clock synchronization in devices, TIIM can struggle with wormhole attacks in

networks, which can reach signals more than the given range of radio or any other section can be defined. Sufficiently tight clock synchronization can be performed in a wireless LAN using commercial GPS receivers [13], and wireless MAN technology could be enough time- synchronized using either GPS or LORAN-C [5] radio signals. Using a TIC, a Mac layer protocol is efficiently protected against replaying, spoofing and wormhole attacks, and assures strong freshness. TIK is implementable with modern technologies and important supplemental processing overhead on MAC layer is not required since the respective packet authentication can be executed on the host CPU.

REFERENCES

[1] Wormhole Attacks in Wireless Networks.pdf

[2] ARC International. ARC releases BlueForm, a comprehensive solution for Bluetooth systems. ARC Press Release 6-04-0

[3] Stefan Brands and David Chaum. Distance-Bounding Protocols. In Workshop on the theory and application of cryptographic techniques on Advances in Cryptology (CRYPTO 1994), volume 839 of Lecture Notes in Computer Science, pages 344–359. Springer-Verlag, August 1994.

[4] Defense Advanced Research Projects Agency. Frequently Asked Questions v4 for BAA 01-01, FCS Communications Technology. Washington, DC. Available at http://www.darpa.mil/ato/solicit/ baa01_01faqv4.doc, October 2000.

[5] Tim Kindberg, Kan Zhang, and Narendra Shankar. Context Authentication Using Constrained Channels. In Proceedings of the Fourth IEEE Workshop on Mobile Computing Systems and Applications (WMCSA 2002), pages 14–21, June 2002.

[6] Ralph Merkle. Protocols for Public Key Cryptosystems. In Proceedings of the IEEE Symposium on Research in Security and Privacy, pages 122–136, April 1980.

[7] David L. Mills. A Computer-Controlled LORAN-C Receiver for Precision Timekeeping. Technical Report 92-3-1, Department of Electrical and Computer Engineering, University of Delaware, Newark, DE, March 1992.

[8] David L. Mills. A Precision Radio Clock for WWV Transmissions. Technical Report 97-8-1, Department of Electrical and Computer Engineering, University of Delaware, Newark, DE, August 1997.

[9] Adrian Perrig, Ran Canetti, Doug Tygar, and Dawn Song. Efficient Authentication and Signature of Multicast Streams over Lossy Channels. In Proceedings of the IEEE Symposium on Research in Security and Privacy, pages 56–73, May 2000.

[10] Proxim, Inc. Datasheet for Proxim Harmony 802.11a CardBus Card. Sunnyvale, CA. Available at http://www.proxim.com/products/all/harmony/docs/ds/harmony_11a_cardbus.pdf.

[11] Amir Qayyum, Laurent Viennot, and Anis Laouiti. Multipoint Relaying: An Efficient Technique for Flooding in Mobile Wireless Networks. Technical Report Research Report RR-3898, Project HYPERCOM, INRIA, February 2000.

[12] Karen E. Sirois and Stephen T. Kent. Securing the Nimrod Routing Architecture. In Proceedings of the 1997 Symposium on Network and Distributed Systems Security (NDSS'97), pages 74–84, February 1997.

[13] Frank Stajano and Ross Anderson. The Resurrecting Duckling: Security Issues for Ad-hoc Wireless Networks. In Security Protocols, 7th International Workshop, edited by B. Christianson, B. Crispo, and M. Roe. Springer-Verlag, Berlin Germany, 1999.

[14] Joseph D. Touch. Performance Analysis of MD5. In Proceedings of the ACM SIGCOMM '95 Conference on Applications, Technologies, Architectures, and Protocols for Computer Communication, pages 77–86, August 1995.

[15] Trimble Navigation Limited. Data Sheet and Specifications for Trimble Thunderbolt GPS Disciplined Clock. Sunnyvale, California. Available at http://www.trimble.com/thunderbolt.html

[16] Akkaya K, Younis M (2005) A survey on routing protocols for wireless sensor networks.
Ad Hoc Networks 3: 325–349.

[17] Eslaminejad M, Shukor AR, Sookhak M, Haghparast M (2011) A review of routing mechanisms in wireless sensor networks.
International Journal of Computer Science and Telecommunications 2: 1–9.

[18] Sohraby K, Minoli D, Znati T (2007) Wireless Sensor Networks: Technology,
Protocols, and Applications. Wiley-Interscience.

[19] Eslaminejad M, Shukor AR, Sookhak M (2012) Classification of energy-efficient routing protocols for wireless sensor networks.
Ad-hoc & sensor wireless networks 17: 103–129.

[20] Detection and Prevention of Wormhole Attack in Wireless Sensor Network using AOMDV Protocol.pd