IJISET - International Journal of Innovative Science, Engineering & Technology, Vol. 1 Issue 2, April 2014.

www.ijiset.com

ISSN 2348 - 7968

Secure and Continuous Wireless Dispatch using Lock-Timeout Puzzles

A. Monika[#1], T. Samraj Lawrence[*2], Dr. R. Ravi[#3]

[#1] *PG Scholar, Department of Computer Science and Engineering, Francis Xavier Engineering College, Tirunelveli, India.*

[*2] *Assistant Professor, Department of Computer Science and Engineering, Francis Xavier Engineering College, Tirunelveli, India.*

[#3] *Professor& Head, Department of Computer Science and Engineering, Francis Xavier Engineering College, Tirunelveli, India.*

Abstract— **The shared nature of any medium in wireless networks makes it easy for an antagonist to launch a Wireless Denial of Service (WDoS) attack. It demonstrates that such attacks can be very easily accomplished using off-the-shelf equipment. A malicious node can continually transmit a radio signal in order to block any legitimate access to the medium and/or interfere with reception. This is called jamming and the malicious nodes are referred to as jammers. Jamming techniques may vary from normal ones based on the continual transmission of interference signals, to more complicated attacks that aim at exploiting vulnerabilities of the particular protocol used. It addresses the trouble of selective jamming attacks in wireless networks. In these attack, the antagonist is alive only for a short period of time, selectively targets messages of high importance To mitigate these attacks, develop three schemes that prevents real time packet classification by combining cryptographic primitives with physical layer attributes and examines the security methods and evaluate their computational and communication overhead.**

Index Terms—Security, jamming, misbehavior, insider attacks, packet dropping.

I. INTRODUCTION

Wireless networks (WN) continue to receive significant concentration as a possible means of providing faultless data connectivity, especially in built-up environments [1]. Generally, such networks evolved from classic mobile ad hoc networks, target long-range transmissions with importance on network throughput and connectivity. WN applications include stationary deployments (e.g., community networks, hierarchal sensor networks) as well as mobile ones (e.g., intelligent transportation system, tactical military networks).

WNs follow two-tier network architecture [2]. The first tier consists of the end users, also referred to as stations (STAs) straightforwardly associated to mesh nodes, referred to as Mesh Access Points (MAPs). The second tier consists of a peer-to-peer network of the MAPs. Connectivity in the second tier is assist by halfway routers known as Mesh Points (MPs) which interrelate MAPs (MPs do not allow connections from end users). The network of MAPs and MPs is often fixed and uses take apart frequency bands to swap over a data and supervise information (MAPs are typically set with multiple transceivers). Lastly, Gateways present connectivity to the wired interactions.

WNs are customarily in danger to "outside" and "inside" attacks. Outside attacks take the forms of random channel jamming, packet rerun, and packet production, and are launched by "foreign" policy that are unaware of the network secret (e.g., cryptographic identification and pseudo-random distribution codes). They are moderately easier to counter through a mixture of cryptography based and healthy communication technique.

In other way, inside attacks, are launched from compromised nodes, are even much more difficult in nature. These attacks develop awareness of network hidden information and protocol semantics selectively and adaptively aim dangerous network functions. Attack selectivity can be received, for sample, by overhearing the primary little bits of a packet [3], or categorization of conveyance based on protocol semantics [4]. Inside attacks cannot be mitigated using only proactive techniques which rely on network hidden information, because the attacker already has access to such hidden information. They moreover need protocols with built-in security actions, through which the attacker can be detected and its selective methods can be exposed.

Security risks of WNs: All types of wireless networks are liable to insider attacks, particularly risks to them, for a number of reasons. Firstly, MPs and MAPs are moderately inexpensive devices with poor physical protection, which makes them possible targets for node trapped and compromise. Secondly, it specified their relatively highly developed hardware. WNs frequently accept a multichannel design, with one or more channels committed for

ISSN 2348 - 7968

manage/transmit purposes. Such inert design makes it as effortless for an attacker to selectively target manage/transmit information. Third, the trust on multi-hop routes accentuates the WMN risks to compromised relays which can crash control information, in order to implement a certain routing performance. It deliberate about several form of complicated attacks in WNs, in which an insider opponent sharply exploits information of leaked cryptographic hidden information and of protocol semantics to attack dangerous network functions such as channel communication, routing, and end-to-end consistent data deliverance. It focus the attention on insider attacks take the form of selective jamming as well as/or else reducing of "high-value" packets in known layer or mixture of layers. While, selective jamming aims at arresting reception during the packet is in transmission, selective reduction is applied for post reception. Next to these, it describes attacks and also high lights detection and mitigation mechanisms.

II. Exploit Attacks

In the world of the wireless medium leaves it at risk to exploit attacks. Security in wireless networks has been primarily analyzed under an outside antagonistic model, as a harsh form of denial of service (DoS). It executes exploit attacks in two multi-hop wireless network schemes. In the first scheme, the attacker embattled a TCP connections establish over a multi-hop wireless route. In the second scheme, the jammer embattled network layer control information transferred during the route establishment process.

A. Exploit attack at the Transport Layer

In the first set of execution, have to setup a file transfer between two users A and B linked via a multi-hop route. The TCP protocol was used to consistently transfer the requested file. The broadcast rate was set to 12 Mbps at each connection. The jammer was located within the nearness of one of the intermediate hops of the TCP link. Four jamming strategies were considered: (a) exploit attacks of cumulative TCP ACKs, (b) exploit attacks of RTS/CTS messages, (c) exploit attacks of data packets, and (d) random attacks of any packet.

It illustrates the number of packets that were jammed by the antagonistic for each value of p. At the end, it shows the fraction of time that the attacks remained active. Here, for exploit jamming attacks, it assumed that 14% of the packet has to be infected in order to be dropped. In the case of random jamming, the antagonistic is not aware of the type of packets transmitted. Hence, they assumed to jam the whole packet in order to drop it. It observes that exploit jamming requires the jamming of accurately one order of magnitude fewer packets than casual jamming. It is because, as the packet transmission speed of the sender drops fewer packets needed to be selectively targeted. Moreover, in exploit jamming, in a fraction of time the antagonist leftovers active is several orders of magnitude less compared to casual jamming. It observes that aiming control packets such as RTS/CTS information and TCP ACKs yields the least jamming activity, because control packets are considerably lesser compared to data packets. Such short attempt jamming attacks are not only well-organized in terms of energy expenses, but also demanding in localizing and essentially removing the jamming devices. Usual methods of transmitter localization such as inward signal strength require that the jamming device leftover active for extended periods of time.

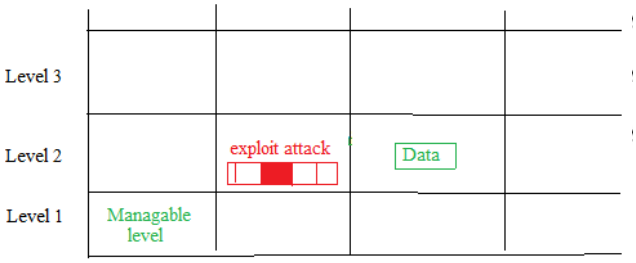

Fig. 1 All Levels during the data communication.

With employing a channel strategy, an inside antagonist can jam only the evasion channel and only during the control phase. Thus the remaining latent follows data transmission stage. This concept is derived in Fig. 1. The impact of this exploit jamming attack propagates to all frequency bands at a small energy overhead, since only a channel is targeted and lone for a fraction of time.

B. Exploit attack at the Network Layer

Numerous anti jamming methods have been proposed to tackle channel exploit attacks from insider nodes. All methods deal transmission efficiency for stronger flexibility to jamming. It gives a short explanation of such anti jamming approaches. Imitation of control information: An instinctive approach to counter exploit jamming is to repeat control information on multiple broadcast channels. In this case, an insider with restricted hardware property cannot jam all broadcasts at the same time. Besides, if each node has only half-done knowledge of the locations on the broadcast channels, an insider can targets the subset of channels alone which is known to antagonist. Owing to the controlled number of available channels, this scheme gives protection against a little number of colluding attackers.

Duty of isolated PN codes: Another method for neutralize channel exploit attacks is to dynamism the position of the broadcast channel, based on the physical position of the communicating nodes. The major inspiration for this structural design is that any broadcast is naturally confined to

ISSN 2348 - 7968

the communication series of the broadcaster. Therefore, for broadcasts planned for receivers in dissimilar collision domains, there is no particular benefit in using the same broadcast channel, other than the design. The assignment of different broadcast channels to different network regions leads to an intrinsic partition of the network into clusters. Messages regarding the position of the control channel in one next cannot be exploited at another. Furthermore, broadcast communication can be repaired close by jammer appear, without the requirements of re-establishing a universal broadcast channel.

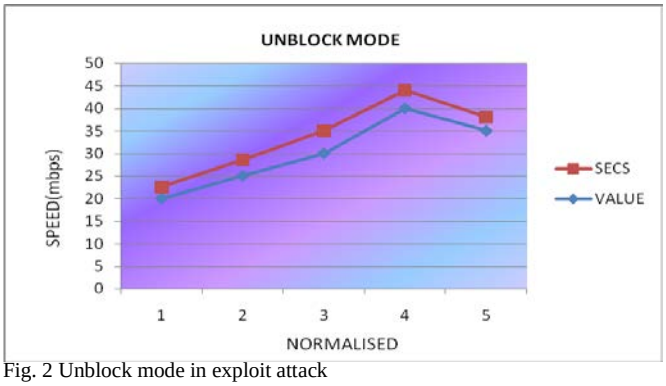

Fig. 2 Unblock mode in exploit attack

Removal of hidden information: Within exploit attacks can be counter by avoid hidden information in the initial place. In [9], a transmitter accidentally selects a unblock mode from open mode. To recuperate a transmit packets, receiver trace the transferred signal and decode it using every unblock mode. Since the unblock mode extends each packet is not identified a initial packet, Surrounded by antagonist can try to supposition it, with a partial chance of success. Unique concern wants to be given to the organization between the transmitting buffers.

In this state, it imitates a multi-hop wireless set of 40 junctions, placed within an allocated area. The normalized routing protocol is mainly used to find out and create routing paths. Association requirements were begin between sender/receiver pairs. It elaborates the number of links established, over the number of links in the lack of the jammers. It exhibits the small amount of seconds that the jammer was alive during the mock-up, for each unblocking strategy. It notices that exploit attack against request information is equally effective to an invariable exploit attack. Moreover, it is explained in the way of selecting attacks which is unsuccessful to disturb the forward detection procedure due to the locking mechanism.

III. LOCK-TIMEOUT/SECS PUZZLES

To recover the power of exploit attacks and decrease the security of identification, invader can work out a higher level of identity by target exact packets of elevated value. The approach of generating an exploit attack is by analyzing packets earlier than their communication is completed.

It suggests a Lock-Timeout/sec Puzzles (LTP), is normally based on similar codes. The major enthusiasm is to accept the lock-timeout technique during the calculation and statement transparency to a least amount. Imagine that the dispatcher D has a packet n for legatee L. Initially, D builds (B, e) = effect (n), where,

$$B = Ie(\phi(n))$$

The consideration function I() is an similar encoding methods, ϕ is a openly recognized variation, and $e \in \{1, 1\}s$ is a arbitrarily certain key of a number of required key extent (the extent of e is a safety limit). The dispatcher telecasts (B||e), "||" indicates the concatenation function. In the lead reaction of e, Legatee L computes

$$n = \phi_1(e(B))$$

Anywhere, ϕ_1^{-1} indicates the inverse transformation of ϕ_1. To accept the lock-timeout technique, the packet containing e is included; such methods of entire bits of e are modified in PHY layer code. To improve e, any legatee can obtain and decipher the final code of the transferred packet, therefore it secure premature leak of e.

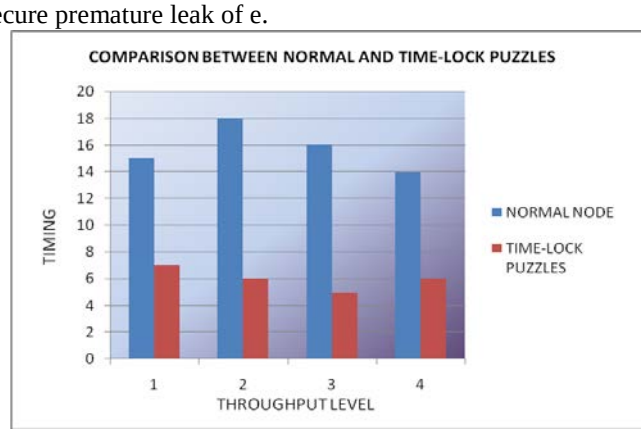

Fig. 3 Throughput level of lock-timeout puzzles.

A. Testing of Lock-Timeout/sec Puzzles

The future TLP needs the combined concern of the PHY layer. To decrease the transparency of TLP, the retreatment value e (i.e., the decryption key) is accepted in the similar packet as the devoted rate B. It stores the exceed packet description essential for transferred e alone. To attain the lock-timeout technique, middle level called the "lock-timeout middle level" is implemented in PHY level. Middle level is in charge for including n earlier than it is process by the PHY level. The functions of the lock-timeout middle level are sketched in Fig. 3.

Packet analyzing can be attained by observes inherent packet selectors such as packet extent, or exact protocol

ISSN 2348 - 7968

locking methods [4]. For example, manageable packets are normally lesser than information packets. The packet extent of well-known communication can be incidental by decodes the system allotment field (SAF) of request-to-send (RTS) and clear-to-send (CTS) communication, used for occupying the wireless medium.

B. Investigation transparency of LTP

Calculating transparency**:** The calculation transparency of LTP is one similar encoding technique at the dispatcher and one similar decoding at the legatee. Since the legend messages are transferred as a promo and embedded, all legatees in the surrounding area of a dispatcher must accept the whole packet and decoded it, prior to the packet variety and objective can be firm. Still, in connectionless protocols the whole packet is arrived at the middle layer earlier than its decision if the packets have to be leftover or be additional process [9]. If various bits of the middle layer header are estimated not to be helpful message to the unblock mode, it may stay unenclosed in the header of the packet, as a result keep away from the decoding methods at the legatee.

IV. EMBEDDED FUTURE KEY

A packet lock system based on embedded future key. The major thought beyond such embedded key is to strength the legatee of a key it performs a predetermined position of computation prior to that it was capable to extort hidden information's interest. The moment essential for getting the key of a problem rely on its inflexibility and the ability of the achiever. The benefit of the key embedded method is defines safety may not be rely on the middle layer parameters.

Key depends on puzzles: Partial achievers can gain major setback value and power expenditure while trade among calculation. In this method, embedded future key can be executed from lock-timeout techniques it normally utilize capable embedded technique. Consumer has a key planned in [10]; utilize single approach puzzle techniques with moderately proceeds an income to make strong key achievers to accurately inhibited range.

A. Testing of embedded future key

The finishing point of the communication S (sec), every legatee can pick up n. As a result, puzzles have to crack and analyze n earlier than the communication value of V has been concluded It has the precautions of Embedded future key at various levels of its implementation.

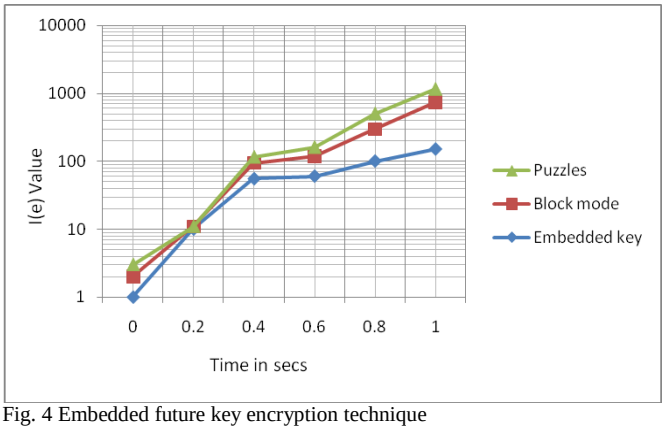

Fig. 4 Embedded future key encryption technique

B. Investigation transparency of embedded future key

Embedded future key: Normally, it is included on the repeated method of an exactly guarded effort of operation. Embedded future key has numerous smart descriptions such as overprotective V and the chronological method of the calculation. Likewise, the future key creations require considerably low calculation compare with embedded key decoding in Fig.4.

V. CONCLUSION

An inside antagonistic form in which embedded key is a part of the system below hit; as a result mortal aware of the protocol terms and common network secrets. It elaborates that the puzzles can analyze conveyed packets in actual time by decrypting the primary secret code of continuing diffusion. It assesses the effect of puzzle timing attacks on system protocols such as ACK and overthrowing. The detection elaborates that an embedded future key can considerably effects on the process of performing a task with extremely small amount of attempt.

REFERENCES

[1] I.F. Akyildiz, X. Wang, and W. Wang. Wireless mesh networks: a survey. Computer Networks, 47(4):445–487, 2005.

[2] Alejandro Proano and Loukas Lazos. Selective jamming attacks in wireless networks. In Proceedings of the IEEE International Conference on Communications (ICC), 2010.

[3] T.X. Brown, J.E. James, and A. Sethi. Jamming and sensing of encrypted wireless ad hoc networks. In Proceedings of the 7th ACM International Symposium on Mobile ad hoc networking and computing, 2006.

[4] J. So and N.H. Vaidya. Multi-channel MAC for ad hoc networks: handling multi-channel hidden terminals using a single transceiver. In Proceedings of the ACM MobiHoc Conference, pages 222–233, 2004.

[5] P. Tague, M. Li, and R. Poovendran. Probabilistic mitigation of control channel jamming via random key distribution. In Proceedings of the International Symposium in Personal, Indoor and

Mobile Radio Communications (PIMRC), pages 1–5, 2007.

[6] L. Lazos, S. Liu, and M. Krunz. Mitigating control-channel jamming attacks in multi-channel ad hoc networks. In Proceedings of the Second ACM Conference on Wireless Network Security (WiSec), pages 169–180, 2009.

[7] Jerry Chiang and Yih-Chun Hu. Cross-layer jamming detection and mitigation in wireless broadcast networks. In Proceedings of the ACM MobiCom Conference, pages 346–349, 2007.

[8] Christina Popper,´ Mario Strasser, and Srdjan Capkun. Jamming-resistant broadcast communication without shared keys. In Proceedings of the USENIX Security Symposium, 2009.

[9] K. Liu, J. Deng, P.K. Varshney, and K. Balakrishnan. An acknowledgment-based approach for the detection of routing misbehavior in MANETs. IEEE Transactions on Mobile Computing, 6(5):536–550, 2007.

[10] W. Kozma and L. Lazos. Dealing with liars: Misbehavior identification via Renyi´-Ulam games. In Security and Privacy in Communication Networks, pages 207–227, 2009.

[11] Han Yu, Zhiqi Shen, Chunyan Miao, C. Leung, and D. Niyato. A survey of trust and reputation management systems in wireless communications. Proceedings of the IEEE, 98(10):1755 – 1772, 2010.

[12] Y. Zhang, W. Lou, W. Liu, and Y. Fang. A secure incentive protocol for mobile ad hoc networks. Wireless Networks, 13(5):569–582, 2007.

[13] Imad Aad, Jean-Pierre Hubaux, and Edward W. Knightly. Impact of denial of service attacks on ad hoc networks. IEEE/ACM Transactions on Networking, 16(4):791–802, 2008.

[14] J. Liu and S. Singh. ATCP: TCP for mobile ad hoc networks. IEEE Journal on Selected Areas in Communications, 19(7):1300–1315, 2002.

AUTHOR(S) PROFILE

A. Monika is presently studying M.E second year Computer Science and Engineering in Francis Xavier Engineering college, Tirunelveli. She has completed her B.Tech Information Technology from SCAD College of Engineering and Technology, Tirunelveli in 2012. Her fields of interest are Networking and Network security.

T. Samraj Lawrence is presently working as a Assistant Professor in the Department of Computer Science and Engineering, Francis Xavier Engineering College, Tirunelveli. He is currently pursuing Ph. D in Wireless Sensor Networks. He has completed his M.E in Computer Science and Engineering from Government College of Engineering, Tirunelveli and B.E in Electrical and Electronics Engineering from Bargur. He has 5years of experience in teaching. His specialization is WSN, Biometrics, and Security.

Dr. R. Ravi is an Editor in International Journal of Security and its Applications (South Korea). He is presently working as a Professor & Head and Research Centre Head, Department of Computer Science and Engineering, Francis Xavier Engineering College, Tirunelveli. He completed his B.E in Computer Science and Engineering from Thiagarajar College of engineering, Madurai in the year 1994 and M.E in Computer Science and Engineering from Jadavpur Government research University, Kolkata. He has completed his Ph.D in Networks from Anna University Chennai. He has 18 years of experience in teaching as Professor and Head of department in various colleges. He published 12 International Journals, 1 National Journal. His areas of interest are Virtual Private networks, Networks, Natural Language Processing and Cyber security