International Journal of Emerging Technology in Computer Science & Electronics (IJETCSE)

ISSN: 0976-1353 Volume 14 Issue 1 –APRIL 2015.

INDRUSION DETECTION IN MANET USING EAACK

S.LAVANYA
Assistant Professor,
Department of Computer science and Engineering,
Sona College of Technology

A.VIJAYAKUMAR,
PG Scholar,
Department of Computer science and Engineering ,
Sona College of Technology,
vijayakumarammasi@gmail.com

ABSTRACT

The migration to wireless network from wired network has been a global trend in the past few decades. The mobility and scalability brought by wireless network made it possible in many applications. Among all the contemporary wireless networks, Mobile Ad hoc NETwork (MANET) is one of the most important and unique applications. On the contrary to traditional network architecture, MANET does not require a fixed network infrastructure; every single node works as both a transmitter and a receiver. Nodes communicate directly with each other when they are both within the same communication range. In the modernization world, the usage of wireless network is more because of their scalability and mobility. MANET is most preferred by many applications because of its infra-structure less network model. The nodes in the network are self configurable. When two nodes comes in a range, they communicate each other. Otherwise the communication is established through the neighbor nodes. These types of open medium of communication have high level of threats and attacks. To avoid this deploy, the intrusion-detection-system mechanisms should protect from attackers. To improve the security, the proposed MANET system can be used into various industrial applications and in emergency situations. In this project, a new advanced secure system can be implemented for MANET. This approach mainly focuses on the intrusion detection and improving the performance of the network. Enhanced Adaptive Acknowledgment and different security methodologies used to protect the network. Compared to contemporary approaches, EAACK demonstrates higher malicious- behavior-detection rates in certain circumstances while does not greatly affect the network performance.

General Terms: Digital signature, digital signature algorithm (DSA), Enhanced Adaptive ACKnowledgment (AACK) (EAACK), Mobile Ad hoc network (MANET).

1. INTRODUCTION

Over the past decade, there has been a growing interest in wireless networks, as the cost of mobile devices such as PDAs, laptops, cellular phones, etc have reduced drastically. The latest trend in wireless networks is towards pervasive and ubiquitous computing - catering to both nomadic and fixed users, anytime and anywhere. Several standards for wireless networks have emerged in order to address the needs of both industrial and individual users. One of the most prevalent forms of wireless networks in use today is the Wireless Local Area Network (WLAN).

In such a network, a set of mobile nodes are connected to a fixed wired backbone. WLANs have a short range and are usually deployed in places such universities, companies, cafeterias, etc. However, there is still a need for communication in several scenarios of deployment where it is not feasible to deploy fixed wireless access points due to physical constraints of the medium. For example, consider communication amongst soldiers in a battlefield, involving troops spread out over a large area. In this case, it is not only feasible to deploy a fixed wireless access point, but also risky since an enemy attack would bring down the whole network. This problem has led to a growing interest among the research community in mobile ad hoc networks, wireless networks comprised of mobile computing devices communicating without any fixed infrastructure. Mobil Ad hoc NETwork (MANET) is a collection of mobile nodes equipped with both a wireless transmitter and a receiver that communicate with each other via bidirectional wireless links either directly or indirectly. Industrial remote access and control via wireless networks are becoming more and more popular these days . One of the major advantages of wireless networks is its ability to allow data communication between different parties and still maintain their mobility. However, this communication is limited to the range of transmitters. This means that two nodes cannot
communicate with each other when the distance between the two nodes is beyond the communication range of their own. MANET solves this problem by allowing intermediate parties to relay data transmissions. This is achieved by dividing MANET into two types of networks, namely, single-hop and multihop. In a single-hop network, all nodes within the

same radio range communicate directly with each other. On the other hand, in a multihop network, nodes rely on other intermediate nodes to transmit if the destination node is out of their radio range. In contrary to the traditional wireless network, MANET has a decentralized network infrastructure. MANET does not require a fixed infrastructure; thus, all nodes are free to move randomly.

However, considering the fact that MANET is popular among critical mission applications, network security is of vital importance. Unfortunately, the open medium and remote distribution of MANET make it vulnerable to various types of attacks. For example, due to the nodes lack of physical protection, malicious attackers can easily capture and compromise nodes to achieve attacks. In particular, considering the fact that most routing protocols in MANETs assume that every node in the network behaves cooperatively with other nodes and presumably not malicious, attackers can easily compromise MANETs by inserting malicious or non cooperative nodes into the network. Furthermore, because of MANET's distributed architecture and changing topology, a traditional centralized monitoring technique is no longer feasible in MANETs.

1.1 MOBILE ADHOC WIRELESS NETWORK*:*

The Mobile Ad hoc Wireless Network is more vulnerable to be attacked than wired network. These vulnerabilities are nature of the MANET structure that cannot be removed. As a result, attacks with malicious intent have been and will be devised *to* exploit these vulnerabilities and *to* cripple the MANET operation. Attack prevention measures, such as authentication and encryption, can be used as the first line of defense for reducing the possibilities of attacks.

However, these techniques have a limitation on the effects of prevention techniques in general and they are designed for a set of known attacks. They are unlikely to prevent newer attacks that are designed for circumventing the existing security measures. The rest of this chapter is organized as follows – initially a classification of wireless networks in use today is described followed by the background and origins of ad hoc wireless networks. The general issues in ad hoc wireless networks are then discussed, followed by a few interesting applications. The final section gives an outline of the chapters to follow.

1.1.1 Taxonomy of Wireless Networks

A wireless network in general consists of a set of mobile hosts which communicate to other mobile hosts either directly or via an access point (base station).The following is a broad classification of wireless networks

1.1.2 Mobile Ad hoc and Sensor Networks

Mobile Ad hoc networks or MANETs are the category of wireless networks which do not require any fixed infrastructure or base stations. They can be easily deployed in places where it is difficult to setup any wired infrastructure. As shown in Figure.1.3, there are no base stations and every node must co-operate in forwarding packets in the network. Thus, each node acts as a router which makes routing complex when compared to Wireless LANs, where the central access point acts as the router between the nodes. A sensor network is a special category of ad hoc wireless networks which consists of several sensors deployed without any fixed infrastructure. The difference between sensor networks and ordinary ad hoc wireless is that the sensor nodes may not be necessarily mobile. Further, the number of nodes is much higher than in ordinary ad hoc networks. The nodes have more stringent power requirements since they operate in harsh environmental conditions. An example of a sensor network is a set of nodes monitoring the temperature of boilers in a thermal plant. Other application domains include military, homeland security and medical care.

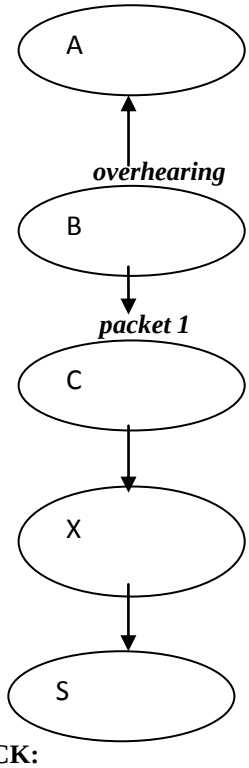
1.1.5 Watchdog

Marti proposed a scheme named Watchdog that aims to improve the throughput of network with the presence of malicious nodes. In fact, the Watchdog scheme is consisted of two parts, namely, Watchdog . Watchdog serves as an IDS for MANETs. It is responsible for detecting malicious node is behaviors in the network. Watchdog detects malicious misbehaviors by promiscuously listening to its next hop's transmission. If a Watchdog node overhears that its next node fails to forward the packet within a certain period of time, it increases its failure counter.

Whenever a node's failure counter exceeds a predefined threshold, the Watchdog node reports it as misbehaving. In this case, the Path rater cooperates with the routing protocols to avoid the reported nodes in future transmission. Many following research studies and implementations have proved that the Watchdog scheme is efficient. Furthermore, compared to some other schemes, Watchdog is capable of detecting malicious nodes rather than links. These advantages have made the Watchdog scheme a popular choice in the field. Many MANET IDSs are either based on or developed as an improvement to the Watchdog scheme. Nevertheless, as pointed out by Marti the Watchdog scheme fails to detect malicious misbehaviors with the presence of the following:

1) ambiguous collisions;
2) receiver collisions;
3) limited transmission power;
4) false misbehavior report;
5) collusion;
6) partial dropping.

Limited transmission power:



1.1.6 TWOACK:

With respect to the six weaknesses of the Watchdog scheme, many researchers proposed new approaches to solve these issues. TWOACK proposed by Liu is one of the most important approaches among them..

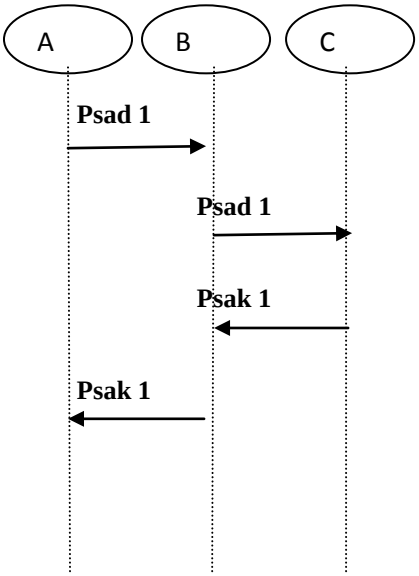
TWOACK scheme:

Each node is required to send back an acknowledgment packet to the node that is two hops away from it. the contrary to many other schemes, TWOACK is neither an enhancement nor aWatchdog-based scheme. Aiming to resolve the receiver collision and limited transmission power problems of Watchdog, TWOACK detects misbehaving links by acknowledging every data packet transmitted over every three consecutive nodes along the path from the source to the destination. Upon retrieval of a packet, each node along the route is required to send back an acknowledgment packet to the node that is two hops away from it down the route.

TWOACK is required to work on routing protocols such as Dynamic Source Routing (DSR). The working process of TWOACK Node A first forwards Packet 1 to node B, and then, node B forwards Packet 1 to node C. When node C receives Packet 1, as it is two hops away from node A, node C is obliged to generate a TWOACK packet, which contains reverse route from node A to node C, and sends it back to node A. The retrieval of this TWOACK packet at node A indicates that the transmission of Packet 1 from node A to node C is successful. Otherwise, if this TWOACK packet is not received in a predefined time period, both nodes B and are reported malicious. The same process applies to every three consecutive nodes along the rest of the route.

The TWOACK scheme successfully solves the receiver collision and limited transmission power problems posed by Watchdog. However, the acknowledgment process required in every packet transmission process added a significant amount of unwanted network overhead. Due to the limited battery power nature of MANETs, such redundant transmission process can easily degrade the life span of the entire network. However, many research studies are working in energy harvesting to deal.

False misbehavior :



1.1.7 AACK:

Proposed a new scheme called AACK. Similar to TWOACK, AACK is an acknowledgment-based network layer scheme which can be considered as a combination of a scheme called TACK (identical to TWOACK) and an end-to-end acknowledgment scheme called ACKnowledge (ACK). Compared to TWOACK, AACK significantly reduced network overhead while still capable of maintaining or even surpassing the same network throughput. The end-to-end acknowledgment scheme in ACK .

1.1.8 Digital Signature

Digital signatures have always been an integral part of cryptography in history. Cryptography is the study of mathematical techniques related to aspects of information security such as confidentiality, data integrity, entity authentication, and data origin authentication The development of cryptography technique has a long and fascinating history. The pursuit of secure communication has been conducted by human being since 4000 years ago in Egypt, according to Kahn's book in 1963. Such development dramatically accelerated since the World War II, which some believe is largely due to the globalization process.

The security in MANETs is defined as a combination of processes, procedures, and systems used to ensure confidentiality, authentication, integrity, availability, and non repudiation Digital signature is a widely adopted approach to ensure the authentication, integrity, and non repudiation of MANETs. It can be generalized as a data string, which associates a message (in digital form) with some originating entity, or an electronic analog of a written signature. Digital signature schemes can be mainly divided into the following two categories.

1) Digital signature with appendix: The original message is required in the signature verification algorithm. Examples include a digital signature algorithm (DSA).

2) Digital signature with message recovery: This type of scheme does not require any other information besides the signature itself in the verification process.

DSA and RSA:

In all of the three scenarios, we witness that the DSA scheme always produces slightly less network overhead than RSA does. This is easy to understand because the signature size of DSA is much smaller than the signature size of RSA. However, it is interesting to observe that the RO differences between RSA and DSA schemes vary with different numbers of malicious nodes. The more malicious nodes there are, the more ROs the RSA scheme produces. We assume that this is due to the fact that more malicious nodes require more acknowledgment packets, thus increasing the ratio of digital signature in the whole network overhead. With respect to this result, we find DSA as a more desirable digital signature scheme in MANETs. The reason is that data transmission in MANETs consumes the most battery power. Although the DSA scheme requires more computational power to verify than RSA, considering the tradeoff between battery power and performance, DSA is still preferable.

1.2 ADVANTAGES OF MOBILE AD HOC NETWORKS:

Having discussed the general issues in MANETs, the reason behind their popularity and their benefits will now be discussed.

(**a) Low cost of deployment:**

As the name suggests, ad hoc networks can be deployed on the fly, thus requiring no expensive infrastructure such as copper wires, data cables, etc.

(b) Fast deployment:

When compared to WLANs, Adhoc networks are very convenient and easy to deploy requiring less manual intervention since there are no cables involved.

(c) Dynamic Configuration:

Ad hoc network configuration can change dynamically with time. For the many scenarios such as data sharing in classrooms, etc., this is a useful feature. When compared to configurability of LANs, it is very easy to change the network topology.

2. EXISTING SYSTEM:

The Watchdog Path rater is a solution to the problem of selfish (or "misbehaving") nodes in MANET. The system introduces two extensions to the DSR algorithm to mitigate the effects of routing misbehavior: the Watchdog, to detect the misbehaving nodes and the Path rater, to respond to the intrusion by isolating the selfish node from the network operation [2]. Intrusion Detection system in MANETS As discussed before, due to the limitations of most MANET routing protocols, nodes in MANETs assume that other nodes always cooperate with each other to relay data. This assumption leaves the attackers with the opportunities to achieve significant impact on the network with just one or two compromised nodes. To address this problem, Intrusion Detection System (IDS) should be added to enhance the security level of MANETs. If MANET can detect the attackers as soon as they enter the network, we will be able to completely eliminate the potential damages caused by compromised nodes at first time. IDSs usually act as the second layer in MANETs, and it is a great complement to existing proactive approaches and presented a very thorough survey on contemporary IDSs in MANETs. In this section, we mainly describe three existing approaches, namely, Watchdog, TWOACK and AACK

TWOACK:

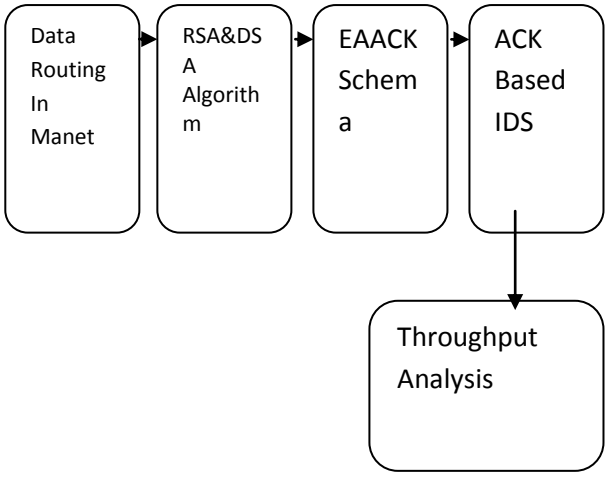
TWOACK is neither an enhancement nor a Watchdog based scheme. Aiming to resolve the receiver collision and limited transmission power problems of Watchdog, TWOACK detects misbehaving links by acknowledging every data packets transmitted over each three consecutive nodes along the path from the source to the destination. Upon retrieval of a packet, each node along the route is required to send back an acknowledgement packet to the node that is two hops away from it down the route. TWOACK is required to work on routing protocols such as Dynamic Source Routing (DSR).

A first forwards packet 1 to node B, and then node B forwards Packet 1 to node C. When node C receives Packet 1, as it is two hops away from node A, node C is obliged to generate a TWOACK packet, which contains reverse route from node A to node C, and sends it back to node A. The retrieval of this TWOACK packet at node A indicates the transmission of Packet 1 from node A to node C is successful. Otherwise, if this TWOACK packet is not received in a predefined time period, both nodes B and C are reported malicious. TWOACK scheme successfully solves the receiver collision and limited transmission power problems posed by Watchdog. However, the acknowledgement process required in every packet transmission process added a significant amount of unwanted network overhead. Due to the limited battery power nature of MANETs, Such redundant transmission process can easily degrade the life span of the entire network.

AACK:

TWOACK Acknowledgement (AACK) similar to TWOACK,AACK is an acknowledgement based network layer scheme which can be considered as a combination of a scheme call ACK (identical to TWOACK) and an end-to-end acknowledgement scheme called ACK. Compared to TWOACK, AACK significantly reduced network overhead while still capable of maintaining or even surpassing the same network throughput. Source node S will switch to TACK scheme by sending out a TACK packet. The concept of adopting a hybrid scheme in AACK greatly reduces the network overhead, but both TWOACK and AACK still suffer from

Existing system diagram:



problem that they fail to detect malicious nodes with the presence of false misbehavior report and forged acknowledgement packets. In fact, many of the existing IDSs in MANETs adopt acknowledgement based scheme, including TWOACK and AACK. The function of such detection schemes all largely depend on the acknowledgement packets. Hence, it is crucial to guarantee the acknowledgement packets are valid authentic. To address this concern, to adopt digital signature in proposed scheme EAACK.

Current node:
If an attacker sends any packet to gather information or broadcast through this system, the Home- Agent calls the classifier construction to find out the attacks. If an attack has been made, it will filter the respective system from the global networks.

Home agent:
It present in each system and it gathers information about its system from application layer to routing layer.

Neighboring node:
Any system in the network transfer any information to some other system, it broadcast through intermediate system. Before it transfer the message, it send mobile agent to the neighboring node and gather all the information and it return back to the system and it calls classifier rule to find out the attacks. If there is no suspicious activity, then it will forward the message to neighboring node.

Data collection:
Data collection module is included for each anomaly detection subsystem to collect the values
of features for corresponding layer in a system. Normal profile is created using the data collected during the normal scenario. Attack data is collected during the attack scenario.

Data process:
The audit data is collected in a file and it is smoothed so that it can be used for anomaly detection. Data preprocess is a technique to process the information with the test train data. In the entire layer anomaly detection systems, the above mentioned preprocessing technique is used. Cross feature analysis for classifier sub model construction.

Local integration:
Local integration module concentrate on self system and it find out the local anomaly attacks.
Each and every system under hat wireless networks follows the same methodology to provide a secure global network.

Global integration:
Global integration module is used to find the intrusion result for entire network. The aim of global integration is to consider the neighbor node(s) result for taking decision towards response module.

3. PROBLEM IDNTIFICATION

My proposed approach EAACK is designed to tackle three of the six weaknesses of Watchdog scheme, namely false misbehavior, limited transmission power and receiver collision. In this section, we discuss these three weaknesses in details. As discussed in previous sections, TWOACK and AACK solve two of these three weaknesses, namely receiver collision and limited transmission power. However, both of them are vulnerable to the false misbehavior attack. In this research work, our goal is to s propose a new intrusion detection system specially designed for MANETs, which solves not only receiver collision and limited transmission power.

4. PERFORMANCE EVALUATION

In this section, we concentrate on describing our simulation environment and methodology as well as comparing performances through simulation result comparison with Watchdog, TWOACK and EAACK schemes.

A. Simulation Methodologies

To better investigate the performance of EAACK under different type of attacks, we propose three scenario settings to simulate different type of misbehaviors or attacks.

1) Scenario 1: In this scenario, we simulated a basic packet dropping attack. Malicious nodes simply drop all the packets they receive. The purpose of this scenario is

to test the performance of IDSs against two weaknesses of Watchdog; namely, receiver collision and limited transmission power.

2) Scenario 2: This scenario is designed to test IDSs' performances against false misbehavior report. In this case, malicious nodes always drop the packets they receive and send back a false misbehavior report whenever it is possible.

3) Scenario 3: This scenario is used to test IDSs' performances when the attackers are smart enough to forge acknowledgement packets and claiming positive result while in fact it is negative. As Watchdog is not an acknowledgement based scheme, it is not eligible for this scenario setting.

5.CONCLUSION

Packet-dropping attack has always been a major threat to the security in MANETs. In this research paper,a novel IDS named EAACK protocol specially designed for MANETs and compared it against other popular mechanisms in different scenarios through simulations. The results demonstrated positive performances against Watchdog, TWOACK, and AACK in the cases of receiver collision, limited transmission power, and false misbehavior report.

Furthermore, in an effort to prevent the attackers from initiating forged acknowledgment attacks, digital signature is incorporated. Although it generates more ROs in some cases, as demonstrated in the experiment, it can vastly improve the network's PDR when the attackers are smart enough to forged acknowledgment packets. This tradeoff is worthwhile when network security is the top priority. In order to seek the optimal DSAs in MANETs, both DSA and RSA schemes is implemented. To increase the merits of this research work, the following issues are planned to investigated in the future work: 1) possibilities of adopting hybrid cryptography techniques to further reduce the network overhead caused by digital signature; 2) examine the possibilities of adopting a key exchange mechanism to eliminate the requirement of redistributed keys; 3) testing the performance of EAACK in real network environment instead of software simulation.

REFERENCES

[1] K. Al Agha, M.-H.Bertin, T. Dang, A. Guitton, P. Minet, T. Val, and J.-B.Viollet, "Which wireless technology for industrial wireless sensor networks?The development of OCARI technol," IEEE Trans. Ind. Electron., vol. 56, no. 10, pp. 4266–4278, Oct. 2009.

[2] R. Akbani, T. Korkmaz, and G. V. S. Raju, "Mobile Ad hoc Network Security," in Lecture Notes in Electrical Engineering, vol. 127. New York: Springer-Verlag, 2012, pp. 659–666.

[3] R. H. Akbani, S. Patel, and D. C. Jinwala, "DoS attacks in mobile ad hoc networks: A survey," in Proc. 2nd Int. Meeting ACCT, Rohtak, Haryana, India, 2012, pp. 535–541.

[4] T. Anantvalee and J. Wu, "A Survey on Intrusion Detection in Mobile Ad Hoc Networks," in Wireless/Mobile Security. New York: Springer- Verlag, 2008.

[5] L. Buttyan and J. P. Hubaux, Security and Cooperation in Wireless Networks. Cambridge, U.K.: Cambridge Univ. Press, Aug. 2007.

[6] D. Dondi, A. Bertacchini, D. Brunelli, L. Larcher, and L. Benini, "Modeling and optimization of a solar energy harvester system for self-powered wireless sensor networks," IEEE Trans. Ind. Electron., vol. 55, no. 7, pp. 2759–2766, Jul. 2008.

[7] V. C. Gungor and G. P. Hancke, "Industrial wireless sensor networks: Challenges, design principles, and technical approach," IEEE Trans. Ind. Electron., vol. 56, no. 10, pp. 4258–4265, Oct. 2009.

[8] Y. Hu, D. Johnson, and A. Perrig, "SEAD: Secure efficient distance vector routing for mobile wireless ad hoc networks," in Proc. 4th IEEEWorkshop Mobile Comput. Syst. Appl., 2002, pp. 3–13.

[9] Y. Hu, A. Perrig, and D. Johnson, "ARIADNE: A secure on-demand routing protocol for ad hoc networks," in Proc. 8th ACM Int. Conf. MobiCom, Atlanta, GA, 2002, pp. 12–23.

[10] G. Jayakumar and G. Gopinath, "Ad hoc mobile wireless networks routing protocol—A review," J. Comput.Sci., vol. 3, no. 8, pp. 574–582, 2007.

[11] D. Johnson and D. Maltz, "Dynamic Source Routing in ad hoc wireless networks," in Mobile Computing. Norwell, MA: Kluwer, 1996, ch. 5, pp. 153–181.

[12] N. Kang, E. Shakshuki, and T. Sheltami, "Detecting misbehaving nodes in MANETs," in Proc. 12th Int. Conf. iiWAS, Paris, France, Nov. 8–10, 2010, pp. 216–222.

[13] N. Kang, E. Shakshuki, and T. Sheltami, "Detecting forged acknowledgements in MANETs," in Proc. IEEE 25th Int. Conf. AINA, Biopolis, Singapore, Mar. 22–25, 2011, pp. 488–494.

[14] K. Kuladinith, A. S. Timm-Giel, and C. Görg, "Mobile ad-hoc communications in AEC industry," J. Inf. Technol. Const., vol. 9, pp. 313–323, 2004.

[15] J.-S. Lee, "A Petri net design of command filters for semiautonomous mobile sensor networks," IEEE Trans. Ind. Electron., vol. 55, no. 4, pp. 1835–1841, Apr. 2008