Hindawi Publishing Corporation
International Journal of Distributed Sensor Networks
Volume 2013, Article ID 184931, 6 pages
http://dx.doi.org/10.1155/2013/184931

Research Article

A Counterattack-Detection Scheme in Transmission Time-Based Wormhole Detection Methods

Dong-uk Kim,[1] Hyo-won Kim,[2] Gisung Kim,[2] and Sehun Kim[1]

[1] *Department of Industrial & Systems Engineering and Graduate School of Information Security, Korea Advanced Institute of Science and Technology, 291 Daehak-ro, Yuseong-Gu, Daejeon 305-701, Republic of Korea*
[2] *Department of Industrial & Systems Engineering, Korea Advanced Institute of Science and Technology, 291 Daehak-ro, Yuseong-Gu, Daejeon 305-701, Republic of Korea*

Correspondence should be addressed to Dong-uk Kim; donguk@kaist.ac.kr

Received 30 August 2012; Revised 7 February 2013; Accepted 27 February 2013

Academic Editor: Dan Kim

Copyright © 2013 Dong-uk Kim et al. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

In recent years, the Mobile Ad hoc Network (MANET) is getting more important and is being utilized in various fields. However, routing-disruption attacks have become a serious problem for MANET. In various routing-disruption attack detection methods, transmission time-based methods can detect wormhole attacks efficiently. Attackers might fabricate a time stamp for a Route Request Packet (RREQ) or Route Reply Packet (RREP) to evade wormhole detection methods. To resolve this weakness, we propose a counterattack-detection scheme in transmission time-based wormhole detection methods. In this paper, we show that it is possible for an attacker to find an effective counterattack against wormhole detection methods, so we provide a counterattack-detection scheme. In the first phase, our proposed method uses the transmission time per hop extracted from a RREQ. If the attackers fabricate the RREQ's starting time to evade our proposed method, we can detect this counterattack using the RREQ's transmission time in the second phase, because the fabricated starting time makes the transmission time shorter than the original transmission time. The simulation shows that our proposed method has high reliability for detecting both wormhole attacks and the attacker's counterattack.

1. Introduction

A Mobile Ad hoc Network (MANET) is a self-configuring network of mobile nodes connected by wireless links. This network can be organized rapidly at low cost and does not require any fixed infrastructure such as fixed routers and backbone. For these reasons, MANET is being utilized in various fields including disaster relief, military operation, emergency service, oil drilling, and mining. In MANET, each node is free to move independently in any direction and can change its links to other nodes. Therefore, the network topology is changeable, and all nodes may enter and exit freely. The connections among nodes are limited to their transmission range, and cooperation with intermediate nodes is required for nodes to forward the packets to other nodes outside their transmission range. These properties compromise the security of MANET, making it vulnerable to attackers. An attacker can modify the routing protocol and disrupt the network operations through mechanisms like packet drops, selective forwarding, and data fabrication. These are called routing-disruption attacks.

One of the most serious routing-disruption attacks is a wormhole attack. These are typically performed by two or more malicious nodes located far from each other. The malicious nodes appear normal but at the same time appear to be within one-hop transmission range. In addition, a wormhole attack can provide fake authenticity and confidentiality, so that other normal nodes perceive the malicious nodes as normal. Therefore, the malicious nodes can form a fake route called a wormhole tunnel that appears to be the shortest legitimate route and then use it to gather network traffic.

To detect routing-disruption attacks including wormhole attacks, researchers have studied several approaches. In sensor networks, routing-disruption attacks can be detected

using authentication techniques such as RSA [1]. If the authentication key is assumed to be secured, these authentication techniques are confidential methods for detecting routing-disruption attacks because an existing attacker cannot use network vulnerability to create a counterattack. However, MANET lacks a centralized administration to manage authentication keys, so that the authentication techniques cannot be applied to detect routing-disruption attacks on a MANET. To resolve this problem, several workers have proposed authentication algorithms for MANET [2–4]. However, these authentication algorithms are not suitable for MANET because of heavy computational requirements and a lack of certain infrastructural elements to support certificates.

In order to avoid using such impractical authentication techniques, the difference in a packet's transmission times has recently been used to detect wormhole attacks [5–7]. Because the transmission time between the wormhole nodes is longer than that between two real neighbors, these methods are simple and do not require heavy computation. In TTM [5], Van Phuong et al. introduced the subject of wormhole attacks on Ad hoc On-demand Distance Vector (AODV) routing protocol in MANET and suggested a time-based detection method using the "Round Trip Time (RTT)" value [8]. The RTT is the time that elapses as a routing packet travels to a remote node and back again, after the route is established. To calculate RTT values, Van Phuong et al. considered the time between sending the Route Request packet (RREQ) and receiving the Route Reply packet (RREP) on every intermediate node. If a route has a considerably longer RTT value, this may indicates that a wormhole link exists between two nodes. Van Phuong et al. also proposed a threshold-based detection rule. This rule decides whether a route has the wormhole link or not by measuring the length of the RTT value of the route.

However, it is difficult to detect abnormal RTT during wormhole attacks because, if attackers know this rule, they can fabricate the time stamp of RREQ or RREP to evade the detection rule. In this paper, therefore, we provide a solution scheme and apply it. In comparison with the work of Van Phuong et al, our contributions are as follows. First, our scheme has a higher attack detection rate, and lower false positive rate, than that of Van Phuong et al. Second, we show that it is possible for attackers to find a counterattack against transmission time-based detection methods described in Tran Van Phuong et al.'s work. Third, we provide a counterattack-detection scheme, unlike Tran Van Phuong et al.'s work.

The remainder of this paper is organized as follows. In Section 2, we describe wormhole attacks on the AODV routing protocol. In Section 3, the proposed method is presented and simulation results are given in Section 4. In Section 5, we suggest the future works and we conclude the paper in Section 6.

2. Wormhole Attacks on AODV

In this section, we describe wormhole attacks on the AODV routing protocol [9]. Since the AODV routing protocol provides a rapid and dynamic network connection, it can be applied to MANET, which has low processing loads and memory consumption.

On AODV, wormhole attacks make use of the RREQ route discovery process, which is based on hop count decrements. Also, wormhole attacks can be launched in two different modes: hidden mode and exposed mode [10]. In these modes, a wormhole node captures RREQs from neighboring nodes and sends RREQs to another wormhole node by means of a wormhole tunnel. The wormhole tunnel can be made by using either an in-band channel or an out-of-band channel [11]. Next, the wormhole node fabricates information about the hop count for the RREQ, and then broadcasts false RREQs to the neighboring nodes. Even though the wormhole tunnel is very long, other normal nodes think that there is only a distance of one hop count. The normal nodes, which receive these false RREQ transmit the reverse route to the sender and update the routing table. Hence, all nodes that receive the false RREQs learn the forged route and subsequently use fabricated information in their data communication.

Briefly, wormhole nodes can gather network traffic using false RREQs and a wormhole tunnel. During the route discovery process, the wormhole nodes can easily reduce the hop count by using either in-band or out-of-band channels, thus depriving a route of accurate data communication. As a result, the other normal nodes believe that the route passing through the wormhole tunnel is the shortest route.

3. Proposed Method

3.1. First Phase: Detection of Wormhole Attacks. In MANET, there is no base station for inspecting packets, so that each node may inspect packets using its own energy and exchange information with neighbors. However, not all nodes have enough energy for such global exchange. Therefore, we selected a feature suitable for identifying the existence of wormhole attacks without the need for exchanging information among neighbors.

For a wormhole attack, the attacker can make a wormhole node using malicious behaviors after entering MANET. First, the wormhole nodes capture RREQs and fabricate the information of the hop count in RREQs. The fabricated RREQs are then sent to another wormhole node by means of a wormhole tunnel, and the received RREQs are broadcast to neighboring nodes. For this reason, the nominal hop count of the fabricated route is shorter than that of other normal routes. That is, the normal RREQ's transmission time, which is the RREQ's elapsed time from starting node to arrival node, is similar to that of the attack RREQ, but their recorded hop counts differ. Accordingly, we propose to use Transmission Time per Hop (TTH), which is the RREQ's elapsed time per hop from starting node to arrival node, as follows:

$$\mathrm{TTH}_{ij} = \frac{C_{ij} - S_{ij}}{H_{ij}}, \tag{1}$$

where i is a node to inspect RREQ, j represents the arrival sequence number of the RREQ on node i, C_{ij} represents RREQ's current arrival time on node i, S_{ij} represents the RREQ's starting time at the origin, and H_{ij} denotes the recorded hop counts of the RREQ on node i. Using this feature in simulation, we confirm that the TTH of the attack RREQ is longer than that of the normal RREQ. The environmental setting is shown in Table 1. Figure 1 presents the TTHs of normal RREQs collected during the target time interval. If this time interval includes wormhole attacks, then the TTH values of the RREQs collected during this time interval may look like Figure 2.

To detect an attack RREQ in real time, each node uses a threshold-based detection rule. The threshold is computed by using the TTH value of normal RREQs, as follows:

$$\text{TTH's Threshold} = \mu + \alpha, \tag{2}$$

where μ is the average TTH of normal RREQs and α represents standard deviation (σ) of the TTH of normal RREQs. In this paper, the threshold is set to $\mu + 2\sigma$ based on outlier detection. The reason for using outlier detection is that it is difficult to set a predefined threshold because MANET is dynamic and unpredictable. Hence, several studies have presented the suitability of outlier detection in MANET [12–14] and researched methods for improving outlier detection in MANET. In the field of outlier detection, the thresholds are usually set to two or three standard deviations from the mean [15]. If a RREQ's TTH is longer than the target threshold, the RREQ is regarded as an attack packet and dropped immediately. Otherwise, the RREQ proceeds to the counterattack-detection phase to verify whether the RREQ is a normal RREQ.

3.2. Second Phase: Detection of Counterattacks. If attackers recognize the proposed wormhole detection method in the network, they may try to find a counterattack against the detection method. One possible counterattack is based on fabrication of the TTH elements by the attackers to reduce the value of TTH artificially, because the TTH of the attack RREQ is longer than that of the normal RREQ. However, attackers cannot fabricate all the elements in calculation of TTH, such as the RREQ's arrival time, starting time, and the recorded hop count. The reason for this is that the RREQ's arrival time, which is not recorded in the RREQ, cannot be collected on an intermediate node and can be only used on the node currently executing the detection method. Also, the recorded hop count has already been changed in order to set the wormhole route. For these reasons, the attackers can only fabricate the RREQ's starting time used in the calculation of TTH, when the RREQ is passed through the wormhole nodes. Figure 3 shows the TTHs of collected RREQs after implementing the simulated counterattack. The environmental setting is shown in Table 1. Note that Figure 3 may look like Figure 1, which presents the TTHs of normal RREQs. As a result, it is possible that the attackers fabricate the RREQ's starting time to reduce TTH artificially.

Table 1: Simulation configuration.

Simulation time	1000 s
Number of mobile nodes	50
Number of wormhole nodes	2
Topology	1500 m × 750 m
Transmission range	250 m
Maximum bandwidth	1 Mbps
Traffic	CBR
Maximum connection	50
Maximum speed	1 m/s

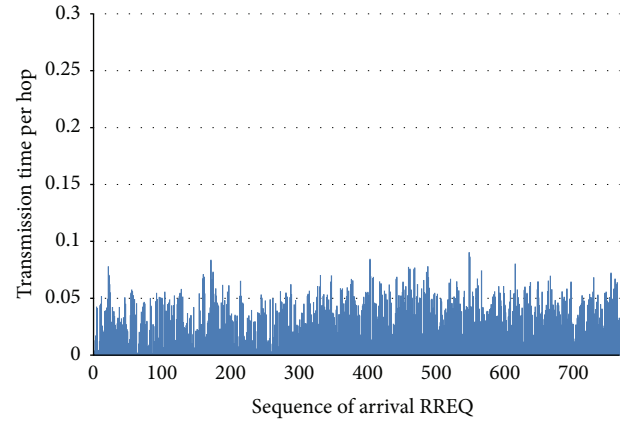


Figure 1: TTHs of RREQs.

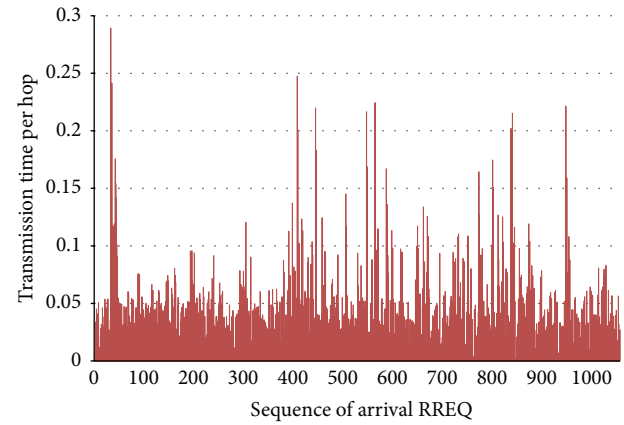


Figure 2: TTHs of attack RREQs.

To detect this attacker's counterattack, we propose to use the Transmission time (T), which is the RREQ's elapsed travel time from starting node to arrival node, as follows:

$$T_{ij}^{k} = C_{ij}^{k} - S_{ij}^{k}, \tag{3}$$

where i is a node to inspect RREQ, j represents the arrival sequence number of the RREQ on node i, k is the origin of RREQ, C_{ij}^{k} represents the RREQ's current arrival time on node i, and S_{ij}^{k} represents the RREQ's starting time at the origin. When a node does not detect wormhole attacks because of

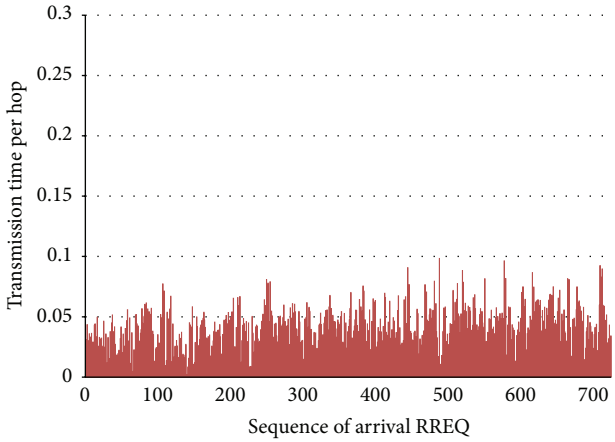


Figure 3: TTHs of collected RREQs after implementation of the counterattack.

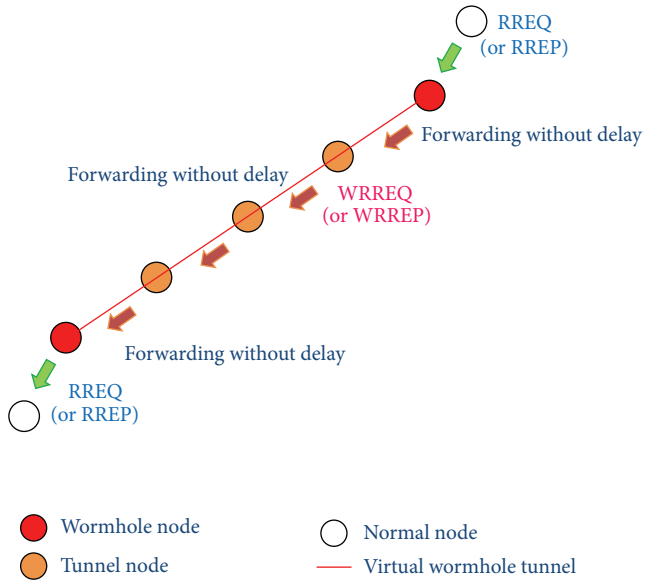


Figure 4: Wormhole tunnel created using WARP [16].

a counterattack, the transmission time becomes shorter than the original transmission time from the same origin because the fabricated starting time is later than the original starting time. Therefore, the node can detect the counterattack using this feature.

To detect such counterattacks in real time, each node must be set to thresholds according to the RREQ origins. The threshold is computed by using the T value of normal RREQs, as follows:

$$T\text{'s Threshold} = \mu - \alpha, \tag{4}$$

where μ is average T of normal RREQs and α represents standard deviation (σ) of T of normal RREQs. In this paper, the threshold is set to $\mu - 2\sigma$ based on outlier detection, as mentioned in Section 3.1. If a RREQ's T is shorter than the threshold of the same origin, the RREQ is regarded as an attack packet and dropped immediately. Otherwise, the RREQ is regarded as a normal RREQ.

3.3. Threshold Updating Procedure. In MANET, the mobility of the node can change the network topology. This may cause changes to the averages of TTH and T. To resolve this, the proposed method is adapted to the changed topology by updating the thresholds. To collect normal RREQs on each node, let us assume that there are no wormhole attacks during the initial time interval just after establishing the network. After each time interval except the initial time interval, the thresholds are updated using normal RREQs of each time interval. The "weighted moving average" method is used for updating the threshold, as follows:

$$\mu_{n+1} = (1 - \alpha)\,\mu_{n-1} + \alpha\mu_n, \tag{5}$$

where μ is the average TTH and T of normal RREQs, n is the current time interval, and α represents the weight of the current average. The α can be changed according to the network environment. In this paper, α is set to 0.5 because this value gives better results from 0 to 1 in our simulation environment. When the "weighted moving average" is calculated in our simulation, the computation time is less than 1 μs. This shows that the "weighted moving average" method requires low computational resources and does not affect the MANET environment.

4. Simulation

We used the NS-2 Network Simulator to evaluate our proposed method. The MANET is assumed to be time-synchronized and constructed for pedestrian speed, because the node speed can be rapid only on a vehicle, and it is then difficult to construct a stable network. In the case of pedestrian speed, the network topology can be changed, but this does not happen frequently. In addition, the network topology is changed slowly, and the threshold updating procedure is performed periodically while changing the topology. In this situation, we established that the threshold updating procedure is performed every 10 seconds. Also, we do not here consider specific network congestion because consideration of such congestion is another research issue. Instead of considering the specific congestion, we simulated our proposed method using random network congestions. Every mobile node was placed randomly and moved according to a random waypoint algorithm [17]. Other details of the simulation configuration are shown in Table 1. The values of these parameters were chosen through reference to other studies [18–20] on MANET.

To generate the wormhole attacks, we used the WARP method [16]. In this method, the WRREQ and WRREP are presented and they refer to the RREQ and RREP in the wormhole tunnel. As shown in Figure 4, the wormhole tunnel was made by several tunnel nodes that executed a special protocol. After receiving an RREQ or RREP on the wormhole node, the wormhole node changes it into a WRREQ or WRREP, which are recognized only by tunnel nodes. In the

Table 2: Detection rates and false positive rates.

	Proposed method		TTM (Van Phuong et al.)	
Time interval(s)	Detection rate	False positive rate	Detection rate	False positive rate
200	93.10%	7.65%	60.00%	11.59%
250	95.00%	6.74%	66.67%	13.40%
300	95.74%	8.19%	66.67%	13.83%
350	96.23%	7.78%	62.50%	13.65%

wormhole tunnel, these packets propagate without delay. When the other end-tunnel node receives a WRREQ or WRREP, the wormhole node changes it back into an ordinary RREQ or RREP. Hence, attack packets have lower hop count than normal packets, and other nodes make reverse routes toward the wormhole nodes.

To execute the attacker's counterattack, we designed the wormhole nodes to fabricate the starting time when the RREQ passed through the wormhole nodes. To reduce the TTH, the fabricated starting time could be calculated by comparing the elements of normal RREQs and those of attack RREQs. That is, we calculated the increased TTH value by fabricated hop count and reduced the TTH value by fabricating the starting time by as much as the increased TTH. Accordingly, the TTHs of attack RREQs were similar to those of normal RREQs.

The initial time interval should be short enough to guarantee that attackers are not in the system. In our simulation, we used 250 seconds as the initial time interval. Following the tradition of other research in this area, the performance of the proposed method was evaluated based on the average detection rate and average false positive rate. When an attacker executes a counterattack against the detection method, the detection rate is reduced from 95.0% to 33.3% and the false positive rate is increased from 6.7% to 11.3%. Hence, we confirm that a counterattack can be performed as we expected. For the purpose of comparison, we conducted simulations at various time intervals comparing TTM [5]. This simulation result is shown in Figure 5 and Table 2. For all time intervals, the proposed method shows higher performance than TTM [5]. Through these results, we validate that our wormhole detection method is also effective in detecting counterattacks.

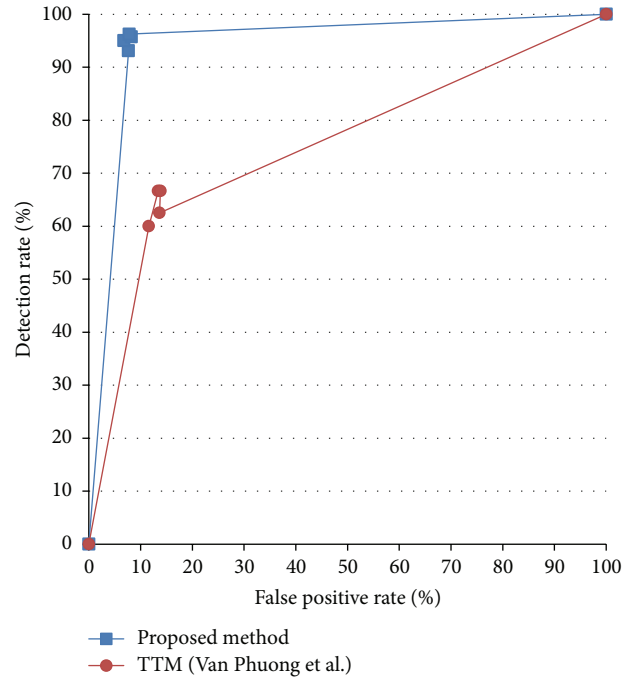


Figure 5: ROC curve for detection performance.

5. Future Work

In the future, we will focus on measuring the detection ratio according to the change in the number of wormhole nodes and detecting the positions of the wormhole nodes. In this paper, we set the number of wormhole nodes at two and the proposed method detects only attack packets. Although, a wormhole attack using two nodes already presents a serious threat to MANET, it is also possible for attackers to increase the number of wormhole nodes. Thus, it is important not only to detect, but also to chase the wormhole nodes and catch the attackers. For these reasons, we intend to extend our proposed method. Additionally, we plan to consider specific congestion issues such as bottlenecks in MANET.

6. Conclusion

In this paper, we have described an attacker's counterattack against a transmission time-based wormhole detection method and proposed a counterattack-detection scheme using the RREQ's transmission time. In order to evaluate our proposed method, we simulated wormhole attacks, detection, and counterattacks, over varying time intervals. Through simulation, we have demonstrated a high probability that the proposed method will be reliable for detecting both wormhole attacks and counterattacks in MANET.

References

[1] R. L. Rivest, A. Shamir, and L. Adleman, "Method for obtaining digital signatures and public-key cryptosystems," *Communications of the ACM*, vol. 21, no. 2, pp. 120–126, 1978.

[2] J. Kong, P. Zerfos, H. Luo, S. Lu, and L. Zhang, "Providing robust and ubiquitous security support for mobile ad-hoc networks," in *Proceedings of the International Conference on Network Protocols (ICNP '01)*, pp. 251–260, November 2001.

[3] S. Capkun, L. Buttyán, and J. P. Hubaux, "Self-organized public-key management for mobile ad hoc networks," *IEEE*

Transactions on Mobile Computing, vol. 2, no. 1, pp. 52–64, 2003.

[4] S. Kaliaperumal, "Securing authentication and privacy in ad hoc partitioned networks," in *Proceedings of the Symposium on Applications and the Internet Workshops (SAINT'03)*, pp. 354–357, January 2003.

[5] T. Van Phuong, N. T. Canh, Y. K. Lee, S. Lee, and H. Lee, "Transmission time-based mechanism to detect wormhole attacks," in *Proceedings of IEEE Asia-Pacific Services Computing Conference (APSCC '07)*, pp. 172–178, December 2007.

[6] F. Nait-Abdesselam, B. Bensaou, and T. Taleb, "Detecting and avoiding wormhole attacks in wireless ad hoc networks," *IEEE Communications Magazine*, vol. 46, no. 4, pp. 127–133, 2008.

[7] Q. N. Dang and L. Lamont, "A simple and efficient detection of wormhole attacks," in *Proceedings of the New Technologies, Mobility and Security Conference and Workshops (NTMS '08)*, pp. 1–5, November 2008.

[8] J. Zhen and S. Srinivas, "Preventing replay attacks for secure routing in ad hoc networks," *Lecture Notes in Computer Science*, vol. 2865, pp. 140–150, 2003.

[9] C. E. Perkins and E. M. Royer, "Ad-hoc on-demand distance vector routing," in *Proceedings of the 2nd IEEE Workshop on Mobile Computing Systems and Applications (WMCSA '99)*, pp. 90–100, February 1999.

[10] M. Khabbazian, H. Mercier, and V. K. Bhargava, "Severity analysis and countermeasure for the wormhole attack in wireless ad hoc networks," *IEEE Transactions on Wireless Communications*, vol. 8, no. 2, pp. 736–745, 2009.

[11] I. Khalil, S. Bagchi, and N. B. Shroff, "LiteWorp: detection and isolation of the wormhole attack in static multihop wireless networks," *Computer Networks*, vol. 51, no. 13, pp. 3750–3772, 2007.

[12] W. Li, J. Parker, and A. Joshi, "Security through collaboration and trust in MANETs," *Mobile Networks and Applications*, vol. 17, no. 3, pp. 342–352, 2012.

[13] W. Li and A. Joshi, "Outlier detection in ad hoc networks using dempster-shafer theory," in *Proceedings of the 10th International Conference on Mobile Data Management: Systems, Services and Middleware (MDM '09)*, pp. 112–121, May 2009.

[14] S. Ganapathy, N. Jaisankar, P. Yogesh, and A. Kannan, "An intelligent system for intrusion detection using outlier detection," in *Proceedings of the International Conference on Recent Trends in Information Technology (ICRTIT '11)*, pp. 119–123, June.

[15] S. Lee, G. Kim, and S. Kim, "Sequence-order-independent network profiling for detecting application layer DDoS attacks," *EURASIP Journal on Wireless Communications and Networking*, vol. 2011, article 50, 2011.

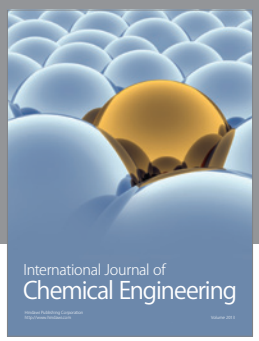
[16] M. Y. Su, "WARP: a wormhole-avoidance routing protocol by anomaly detection in mobile ad hoc networks," *Computers and Security*, vol. 29, no. 2, pp. 208–224, 2010.

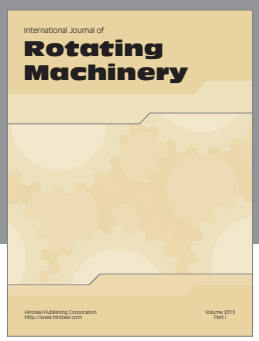
[17] C. Bettstetter, G. Resta, and P. Santi, "The node distribution of the random waypoint mobility model for wireless ad hoc networks," *IEEE Transactions on Mobile Computing*, vol. 2, no. 3, pp. 257–269, 2003.

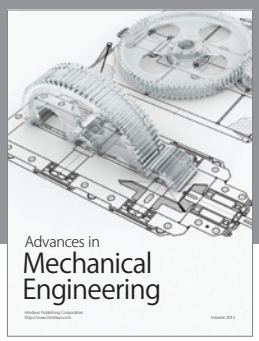
[18] G. Kim, Y. Han, and S. Kim, "A cooperative-sinkhole detection method for mobile ad hoc networks," *AEU*, vol. 64, no. 5, pp. 390–397, 2010.

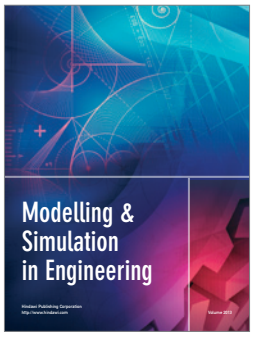
[19] Y. C. Hu, D. B. Johnson, and A. Perrig, "SEAD: secure efficient distance vector routing for mobile wireless ad hoc networks," *Ad Hoc Networks*, vol. 1, no. 1, pp. 175–192, 2003.

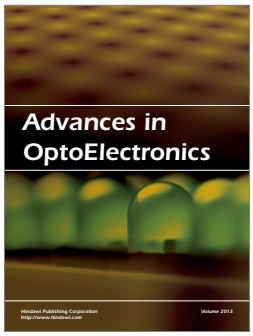
[20] A. P. Emmanouil, N. Levon, and P. Christos, "Securing AODV against wormhole attacks in emergency MANET multimedia communications," in *Proceedings of the 5th International ICST Mobile Multimedia Communications Conference (Mobimedia '09)*, article 34, September 2009.

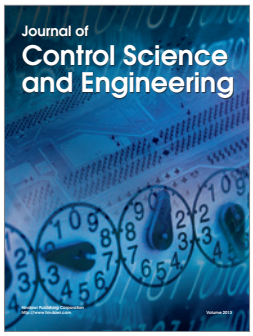


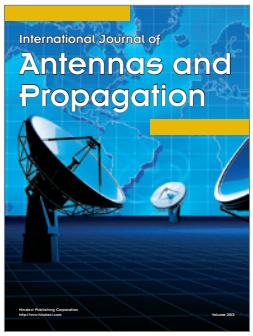


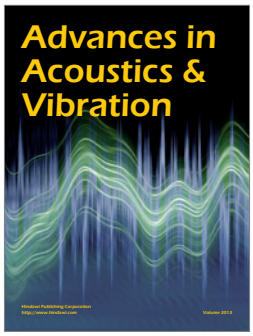


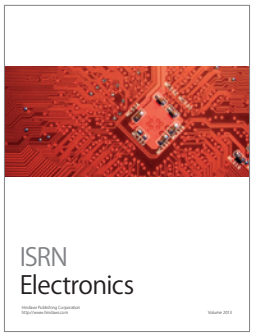
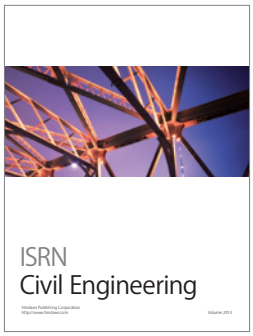
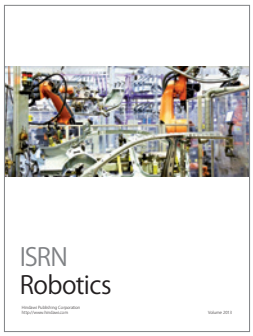
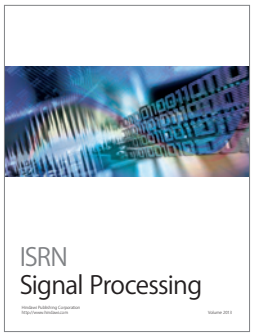
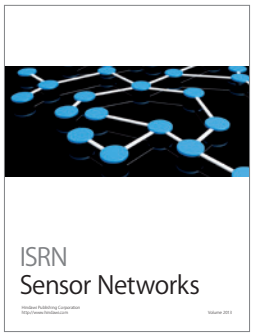
Hindawi
Submit your manuscripts at
http://www.hindawi.com











ISRN
Electronics

ISRN
Civil Engineering

ISRN
Robotics

ISRN
Signal Processing

ISRN
Sensor Networks