AU J.T. 10(4): 215-224 (Apr. 2007)

Dynamic *K*-value for Belief-based Ad Hoc Sinkhole Detection

Piyakul Tillapart, Tapanan Yeophantong, Patra Vatanasak, and Sahapak Manopimok

Faculty of Science and Technology, Assumption University
Bangkok, Thailand

Abstract

Sinkhole detection is one of the challenging issues in the area of ad hoc network security, since a sinkhole attack disrupts communications in the entire network by attracting traffic to a malicious path of the network. However, transmission failure in the ad hoc network is caused not only by the sinkhole attack but also by weak signal strength which forms a communication link. In practice, ad hoc nodes are located in different places where their environmental conditions may be different. These environments affect nodes' signal strength which would affect success of packet transmission between nodes. If a node is located in a bad environment, the node maintains poor communication links with its neighboring nodes, causing high probability of packet loss. Consequently, this innocent node becomes less trusted by its neighbors and may eventually be classified as a sinkhole. In this research, we present an approach for sinkhole detection in ad hoc networks in poor environment.

Keywords: *Sinkhole detection, ad hoc network, belief-based detection mechanism, and dynamic network environment.*

1. Introduction

A mobile ad hoc network is an infrastructureless network which is temporarily formed up from a collection of two or more mobile nodes. The nodes are capable of transmitting data packets through wireless links. The network topology is not fixed since the nodes are free to move and are allowed to join and leave the network at any time. Due to the limited transmission range of wireless links, the nodes within each other's wireless transmission range can communicate directly while distant nodes located outside their transmission ranges have to relay messages through neighboring nodes. Therefore, each node operates not only as a host when receiving/sending data from/to other nodes but also as a router when being dynamically involved in the path set up between other nodes in order to transmit data packets to arbitrary destinations (Deng *et al*. 2002; Ramaswamy *et al*. 2003; Burg 2003).

Characterized by the dynamic nature of the network topology, open medium, absence of central support infrastructure, distributed cooperation, and constrained transmission capability, the ad hoc networks are more vulnerable to various types of attacks such as eavesdropping, injected bits, fake route reply, and malicious routing attacks. By attacking routing protocols, an attacker can introduce a malicious node into a routing path between a source-destination pair in the network. Consequently, the malicious node can later drop or alter attracted data packets and generate fake route replies.

In this paper, we emphasize on a sophisticated routing attack called sinkhole attack which is a challenging issue in ad hoc network security. A sinkhole attack is caused by a malicious node which lures traffic to a malicious path of the network. The malicious node exploits an ad hoc routing protocol and attracts its neighbors by answering each route request with a fake route reply claiming to have the best path to a given destination. Therefore,

ordinary nodes start sending data packets to the destination through the sinkhole which prevents the destination from obtaining complete and correct data. Thereafter, the attack can gain access to the biggest part of data flowing through the network and may disrupt communications in the network. Finally, it can form up a serious threat to high-layer applications (Burg 2003; Wu *et al*. 2005; Kapil and Ghosh 2005).

Unfortunately, disrupted communication in the ad hoc network may be caused not only by the sinkhole attack but also by link interferences between communicating nodes. Since the transmission link between communicating nodes is a wireless link, it becomes susceptible to inferences like other signal frequencies, solid obstacles, and environmental conditions. Moreover, it also gets attenuated over distance. For instance, if an ordinary node in a routing path is unfortunately located in poor environment such as heavy raining condition or thick-walled room, the signal strength of the link between the node and its neighboring node may be weak. Therefore, the node may become unable to receive/forward data packets from a sending neighboring node/to a next hop in the path. When a certain number of data packets could not be delivered to the destination, the innocent node which now could not participate in data forwarding is incorrectly detected as a sinkhole. This fault detection would cause high fault positive rate in the intrusion detection system.

In this paper, we enhance an earlier work, the trust-based sinkhole detection (Thanachai *et al*. 2006), by introducing a dynamic *K*-value for belief-based sinkhole detection where the *K*-value indicates the environmental conditions along the routing path between source and destination. If a node is located in a poor environment, then the node has an increased probability to fail the data forwarding process and may soon be considered as a sinkhole. In the proposed method, every node in the network considers the signal strength between directly connected neighbors which is affected by the environmental conditions. Consequently, the proposed method yields good performance of sinkhole detection with low fault positive rate, indicating that the innocent nodes located in poor environment are not detected as sinkholes.

The remaining part of this paper has been organized into several sections. Section 2 provides information related to existing research works on sinkhole detection. Section 3 considers the trust-based sinkhole detection. Section 4 describes the proposed method followed by the computational results and analysis in Section 5. Lastly, Section 6 draws a final conclusion.

2. Related Works

The routing attack, especially the sinkhole attack, is not only an important issue of ad hoc network security, but also disrupts the communications in the network. Therefore, the implementation of an ad hoc network in a large scale in the presence of sinkholes is a difficult task. This problem is now pulling researchers attractions. Ad hoc network security mechanisms can be classified into two approaches, intrusion prevention and intrusion detection and response technology. The intrusion prevention technology is based on authentication, encryption and key management (Zhou and Haas 1999; Kurian 2004; Frankel *et al*. 1997; Herzberb *et al*. 1997; Akosan and Ginzboorg 2000; Khalili *et al.* 2003). A message from the source must be encrypted with a secret key before being sent to the destination. Consequently, the message is decrypted by the destination before being read. However, authentication-based and cryptography-based security mechanisms may be difficult to accomplish in an ad hoc network due to an absence of any central support infrastructure as well as the consumption of more energy which is an important concern in ad hoc networks (Ramaswamy *et al*. 2003; Chen *et al*. 2006).

The second approach, using an intrusion detection system (IDS), attempts to identify intruders by detecting suspicious activities that occur within the system. The intrusion detection systems can broadly split into two classes based on reputation-based and incentive-based approaches, correspondingly. According to the reputation-based approach, a

mobile node will be punished or avoided during routing when the node misbehaves or does not properly relay data to the destination. On the other hand, positive promotion will be given to the node in order to encourage the node to forward data. Recently, many researchers have been attracted to develop IDS that can identify and resolve sinkhole attacks in ad hoc networks.

Watchdog was proposed by Marti *et al*. (2000) to mitigate the presence of a sinkhole problem in the network. The proposed method is an extension of the Dynamic Source Routing protocol (DSR). To identify a misbehaving node, a sending node promiscuously listens to next node's transmission. If the next node does not forward the packet, then it is misbehaving. However, the watchdog is vulnerable to attacks from two consecutive and colluding adversaries where the first adversarial node does not report that the second one did not forward the data.

Deng *et al*. (2002) and Ramaswamy *et al*. (2003) discussed the problems with the *ad hoc* on demand distance vector routing protocol (AODV). Deng *et al*. (2002) proposed a solution to identify a single sinkhole in a network. In the proposed solution, the AODV protocol is slightly modified to carry necessary next hop information. After the source receives the route information to be used for data forwarding form a neighboring node, the source will not immediately transmit a data packet through the available path. Instead, the source sends an additional message to the next hop to verify that it has a route to the intermediate node. If the next hop has no route to the requested intermediate node and it also has no route to the destination, the source suspects the intermediate node and then sends out an alarm message to isolate the malicious node. Unfortunately, the proposed solution cannot be applied to identify a cooperative black hole attack involving multiple nodes. Ramaswamy *et al*. (2003) presented a modified solution in order to identify the cooperative black hole attack. The modified solution makes use of the Data Routing Information table which contains a trusted nodes list and Cross Checking. The identification method in the modified solution does not depend only on the route information but also on the nodes' transmission history. The source node transmits data packets only through the trusted nodes with good transmission histories. If the source node doesn't have enough history of the intermediate nodes then the source node will send further a request message to the next hop after the intermediate node in order to identify the trustworthiness of the said intermediate node.

Kapil and Ghosh (2005) presented a sinkhole detection method which uses a backbone network of strong nodes over the initial ad hoc network. The strong nodes are powerful in terms of computing power and radio range and are assumed to be trustful and responsible for the monitoring of traffic being forwarded through regular nodes. Thus, the backbone network is used for hierarchical routing where the backbone is placed at a higher level for monitoring the traffic in the ac hoc network. Therefore, a source node can check whether the data packets have reached their respective destination or not with the assistance of the strong nodes.

A trust evaluation scheme based on clustering was proposed by Jin *et al*. (2005) to secure an ad hoc network against sinkhole attacks. In this scheme, a cluster is created by neighboring nodes. Then a node in the cluster with the highest trust value will be elected as a cluster head. The cluster head acts as a trust guarantor and will issue trust value certificates to cluster members upon request. A member node uses the certificate to show its trustworthiness when communicating with other nodes. Also, a node evaluates the trust of another node based on both the node's own experience and information in the certificate. Even in the case that a node has no experience, it can evaluate other nodes with regard to the cluster head's information. Therefore, the node does not have to store and manage experience data about all the other nodes in the network. Unfortunately, if the cluster heads have been attacked then the network will be in chaos.

A recent work, trust-based ad hoc sinkhole detection (Thanachai *et al*. 2006), is a fully distributed method. Initially, every node assigns trust-weight to its neighbors. During the transmission, if a neighbor fails to relay its message to a designated receiver, the node then

reduces the trust-weight it has given to the neighbor. The neighbor then subsequently decreases the assigned weight of the next ad hoc node in the transmission path. Once the trust-weight of any neighbor falls below a specified threshold, then the neighbor is treated as a suspicious node. The ad hoc node will then consult with its other neighbors in order to find out whether or not the suspicious node should be identified as a malicious node. The approach itself yields a great advantage, since it does not require any centralized unit to make the decision, and allows the ad hoc node to make the decision solely by itself.

3. The Trust-Based Sinkhole Detection Mechanism

The trust-based sinkhole detection (TBD) (Thanachai *et al*. 2006) allows every ad hoc node in the network to assign trust-weight to its neighboring nodes. The trust-weight is used to determine the most trusted communication path between source and destination. The current path can be replaced by an alternative path in case the current path becomes less trusted during the routing process. The neighbor's trust-weight is increased or decreased when the node successfully or unsuccessfully transmits the information packets. If the weight is lower than a specified threshold, the suspicious node will be classified automatically as a sinkhole node.

In TBD, there are 4 main processes: route selection, belief adjustment, history list, and detection mechanism.

3.1 Route Selection

When a source node has to deliver a message to a given destination, the source performs a route selection process toward the destination by broadcasting a route request message (RREQ) to the destination and waits for a route reply message (RREP) from the destination. There might be a number of RREP messages sent back from the neighboring nodes since there are many paths available. Then the source node chooses the best path based on a path's route weight (R) in which the path's route weight is also depended on a trust-weight the source has given to the neighbor. To avoid malicious path selection, the source will choose the path through the neighbor which gives the best route weight:

$$R_i = h_i * (1 - W_{s \to i}), \quad (1)$$

where i is the neighbor i, s is the source, R_i represents the route weight of the node i, h_i is the number of hops from node i to the destination, and $W_{s \to i}$ is the trust-weight of node i assigned by the source node (the initial trust-weight is 1.0).

3.2 Belief Adjustment

After the path has been selected, the source starts transmitting messages through the chosen neighbor. Then the neighbor relays messages along the path. When the source node transmits a message through its' neighbor, it waits for an acknowledgement (ACK) message from the destination. If it receives the ACK from the destination, it will increase the trust-weight it has given to the neighbor; otherwise the neighbor's trust-weight will be reduced by the value of weight adjustment (WA_i):

$$WA_i = \frac{1}{Kn_i}, \quad (2)$$

where i is a next hop index, n_i is the number of hops between node i to the destination node, and K is the environmental constant of the transmission path.

According to Eq. 2, the node which is located near to the destination will significantly decrease the neighbor's trust-weight while the node which is far from the destination will slowly reduce the trust-weight of its neighbor. Based on the sinkhole characteristics, it is assumed that sinkhole nodes advertise the shortest path to the destination. Therefore, if the neighbor is a sinkhole then the trust-weight of the sinkhole will be reduced rapidly.

After the node adjusts the neighbor's trust-weight, it then broadcasts a weight adjustment message to other neighboring nodes. The message is used to inform other neighbors that the sending node believes that the trust-weight of the neighbor is a subject of change. Then other neighbors examine whether they have ever worked with that neighbor. If

they have ever worked with it, they will also adjust their trust-weight by the value of W' as shown in the following formula:

$$W'_{A\to C} = \frac{t_A}{T}\left(\left(\frac{2W_{A\to A}}{W_{A\to A}+W_{A\to B}}\right)*W_{A\to C}\right) + \frac{t_B}{T}\left(\left(\frac{2W_{A\to B}}{W_{A\to A}+W_{A\to B}}\right)*W_{B\to C}\right), \quad (3)$$

where $W_{i\to j}$ represents the weight i gives to j, T_n represents the number of transmissions between node n and the suspicious node, and T represents the sum over T_n.

3.3 History List

Each ad hoc node has its own database for storing a list of neighboring nodes and nodes that it has worked with before. The history list consists of ID and trust-weight of the past and the present neighbors. The list also helps during the trust-weight initialization process.

When a new node joins the network and becomes a neighbor of existing nodes, the existing nodes will check their history list to examine whether they have worked with the newcomer. If they had worked with the node before, then they will assign to the new node the latest trust-weight recorded in the history list.

3.4 Detection Mechanism

In any ad hoc node, if any neighbors' trust-weight in the history list is lower than the specified threshold, the neighbor is being classified as suspicious. Then the node broadcasts an inspection request message to other neighboring nodes which may have information about the suspicious node. If they have worked with the suspicious node before, they reply back to the requesting node. Then, the node determines the inspection weight, W. If the inspection weight is lower than a specified threshold, then the requested node identifies the suspicious node as a sinkhole node:

$$W_i = \frac{\sum(W_{\text{In}\to\text{Neighbor}} * W_{\text{Neighbor}\to\text{S}})}{\sum W_{\text{In}\to\text{Neighbor}}}, \quad (4)$$

where W_i represents the inspection weight, $W_{\text{In}\to\text{Neighbor}}$ represents the trust-weight the node (which initiates the inspection request) gives to its neighbor, and $W_{\text{Neighbor}\to\text{S}}$ represents the trust-weight the neighbor node gives to the suspicious node.

3.5 Problem Statements

In TBD, the K-value is an environmental constant having a fixed value for every node in the entire network. Therefore, every node is provided with a certain probability to fail its transmission. For instance, let an ad hoc node send a packet to the destination through a particular neighbor. If the transmission fails and the hop count from the neighbor to the destination (n) is 2 when the environmental constant K equals 2, then the node reduces the trust-weight of its neighbor from 1 to 0.75. As a result, the K-value provides the ad hoc nodes with chances to prove themselves before the trust-weight reaches the specified threshold of 0. If the K-value is too high, the speed of sinkhole detection is slow due to the many chances given to each node in the network. Conversely, if the K-value is too low, then the speed of sinkhole detection is fast because little chances are given to each node in the network. Improperly assigned K-values lead to either positive high-fault rates or slow detection rates.

In practice, the environmental conditions over all transmission links between the communicating nodes are not the same and are often unstable. These environmental conditions include distant nodes, solid obstacles, weather conditions, e.g., raining, etc. In such cases, an ordinary node may be unable to relay messages to the corresponding destinations because of the poor physical environment.

4. The Proposed Method

In this paper, we present an approach for distinguishing innocent nodes located in poor environment from actual sinkholes. Following a recent work on trust-based ad hoc sinkhole detection (Thanachai *et al*. 2006), we improve the technique with a mechanism to allow a dynamical adjustment of the "environmental constant," or K-value, defined in Thanachai *et*

al. (2006). In our approach, a node in the network maintains *K*-values of a transmission link to its neighbor. If a node can detect high level signal of the neighbor's signal strength, the node assigns a low number to the *K*-value; otherwise the *K*-value will be set to a high value. Thus, the *K*-value is dynamically adjusted on the basis of the changing environment in which the nodes are located. In the proposed method, every node in the network considers the directly connected neighbors' signal strength which depends on the environmental conditions. The idea of the proposed method is that if a node is located in bad environment, the node has a higher probability to fail the packet transmission process. With the dynamic *K*-value, the method consequently achieves a high sinkhole detection rate with low false positive rate despite the poor environmental conditions.

In the proposed method, ad hoc nodes participate in the four main processes as described in Section 3. However, the first two processes adopt the dynamic *K*-value in order to operate in a dynamic environment.

4.1 Signal Strength, *K*-Value, and Packet Loss

When a source node sends a route request message to a destination node and a number of paths are available, then the node receives RREP messages from its neighboring nodes. According to the received RREP messages from its neighbors, the source selects a path to the destination based on the route selection formula shown in Eq. 1. Then the source measures the signal strength of its neighbor and assigns a *K*-value to its neighbor. For different levels of signal strength, different *K*-values are assigned. The higher the signal strength, the lower is the *K*-value. The source periodically maintains the *K*-value to reflect the signal strength of its neighbors.

In this research, the signal strength is divided into five levels. Level 5 means that a node detects a strong signal from its neighbor while Level 1 indicates that a node detects a weak signal from its neighbor. The signal strength between a node and its neighbor depends on factors such as distance, obstacles, and environmental conditions. For example, if there are solid obstacles between the nodes, then the signal strength decreases. The signal strength reflects the percentage of packet loss. When the signal strength is high, the percentage of packet loss is low. On the contrary, the percentage of packet loss is high when the signal strength is weak. The assumed relations between the signal strength and the percentage of packet loss are shown in Table 1.

4.2 Dynamic *K*-Value Adjustment

We introduce two comparative approaches for the use of the dynamic *K*-value during the belief adjustment process:

- AVG-*K* approach: An average *K*-value is obtained from all the *K*-values of the communication links in the route from source to destination.
- MAX-*K* approach: A maximum *K*-value is obtained from all the *K*-values of the communication links in the route from source to destination.

We use these strategies rather than assigning different *K*-values to each communication link in the route because a node knows only the environmental conditions in its neighborhood. For instance, if the environment around a node is good, the node may assign a quite low *K*-value to its neighbor in the path, not knowing that, perhaps, the environmental conditions are worse elsewhere along the route. Consequently, this causes the node to unnecessarily punish its neighbor.

Table 1. Relation between signal strength and probability of packet loss.

Signal Strength	Probability of Packet Loss
5	0
4	1/3
3	1/2
2	2/3
1	1

5. Computational Experiments

Computational experiments can be conducted to test the proposed dynamic *K*-value method versus the trust-based sinkhole detection (TBD) with constant *K*-value.

5.1 Computational Set-up

Our sample network is composed of 49 nodes arranged in a grid pattern of 7×7 nodes.

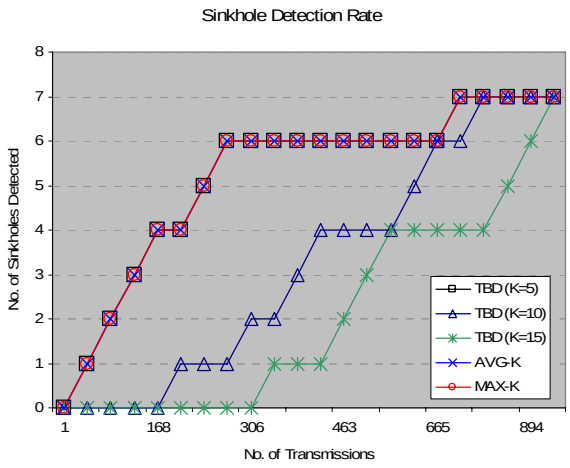
During every computational experiment, one thousand transmissions (packets) are scheduled for transmission between source and destination. The source and the destination are located on the left-most and the right-most column of the network metric. Seven malicious nodes are randomly placed into the network. Also, the environmental conditions of the network are dynamically changed on the basis of two parameters, ECR and ETR.

The Environmental Change Rate (ECR) reflects the probability of environmental change. The nature of the change, positive or negative, depends on the Environmental Turbulence Rate (ETR), which reflects the probability of negative environmental change. For instance, a sample network with ECR = 33 and ETR = 75 means that there is 0.33 probability for the environment of the area to change with 0.75 probability the changes to be negative.

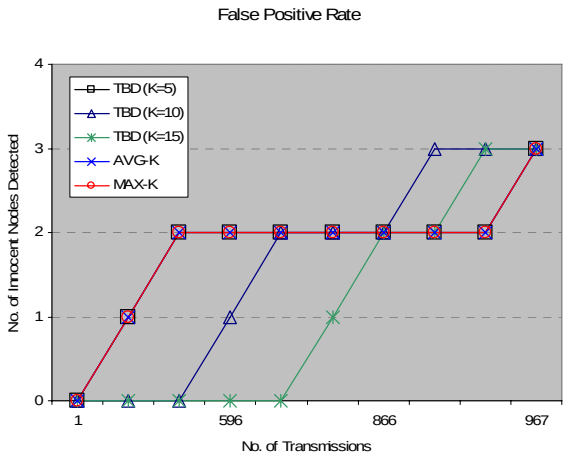
Several network scenarios are tested to compare the original TBD approach to the proposed method. In TBD, approaches with varying constant *K*-value of 5, 10, and 15 are tested. In the proposed method, the average *K*-value (AVG-*K*) and maximum *K*-value (MAX-*K*) approach are tested. Each node sets a trust-weight of 1.0 to all neighboring nodes in the network during the data initialization.

5.2 Computational Results and Analysis

The results of computational experiments are shown in Figs. 1–4. Varying values of ECR and ETR are used in order to simulate dynamic environmental conditions during the data transmission between source and destination.



(a)



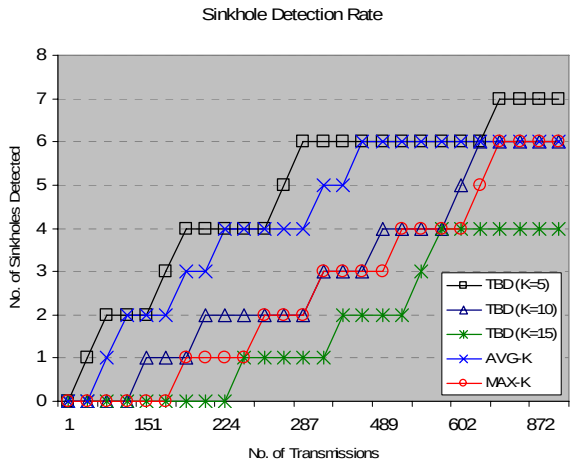
(b)

Fig. 1. (a) Sinkhole Detection Rate and (b) False Positive Rate (ECR = 0, ETR = 0, and 7 sinkholes).

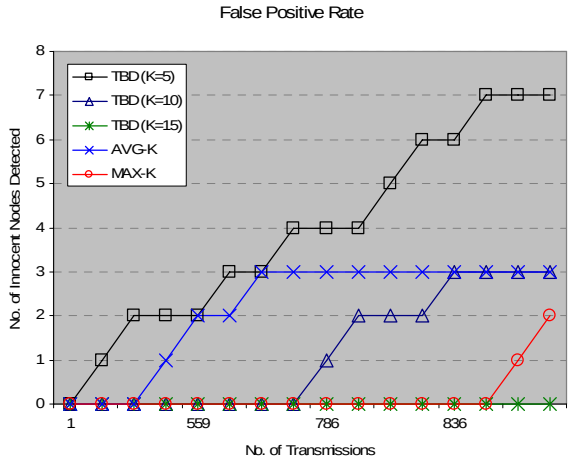
The computational results in Fig. 1(a) show the sinkhole detection rate when the dynamic environmental parameters (ECR and ETR) are being set to zero. The zero values indicate that the ad hoc nodes are located in good environment with no obstacles and no changes in the environmental condition. The results show that TBD (*K*=5), AVG-*K*, and MAX-*K* give both the same sinkhole detection rate and false positive rate because the network environmental condition remains good and unchanged and the *K*-values used in AVG-*K* and MAX-*K* approach are identical to TBD (*K*=5). Since the *K*-value is low, the nodes are given a few chances to fail the transmission. Therefore, the sinkholes would be detected quickly. Apparently, a few innocent nodes, which are located near to the sinkholes, are affected by the sinkhole attacks. As shown in

Fig. 1(b), a few innocent nodes are incorrectly classified as sinkholes.

Figs. 2–4 show the computational results when the network environmental condition is changed with variation of ECR and ETR values. The results show that AVG-*K* and MAX-*K* approaches can detect sinkholes in the network at almost the same rate, except TBD (*K*=5) because the TBD (*K*=5) approach uses the constant *K*-value of 5, therefore, the sinkholes would be detected rapidly. In addition, TBD (*K*=10) and TBD (*K*=15), use high *K*-values. Therefore, the nodes are given higher chances to survive in the network. AVG-*K* and MAX-*K* also use large *K*-values in the belief adjustment process.

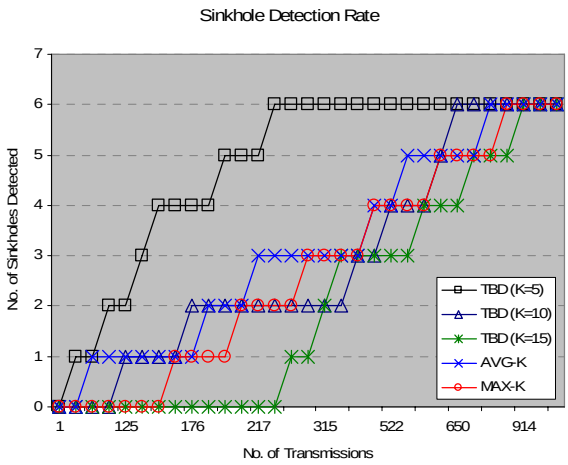


(a)

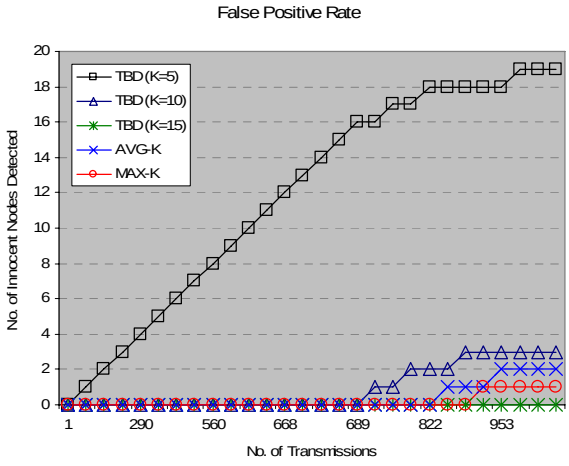


(b)

Fig. 2. (a) Sinkhole Detection Rate and (b) False Positive Rate (ECR = 33, ETR = 50, and 7 sinkholes).



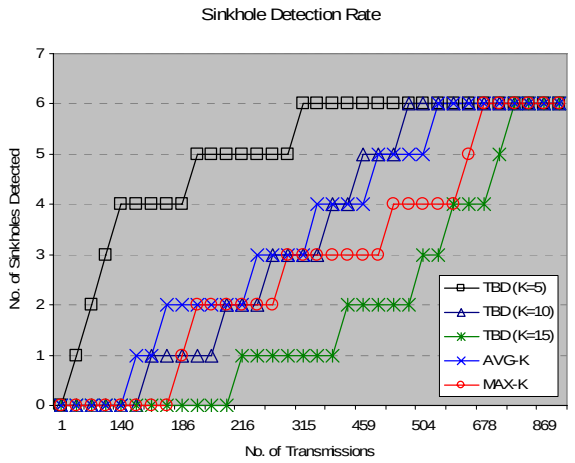
(a)



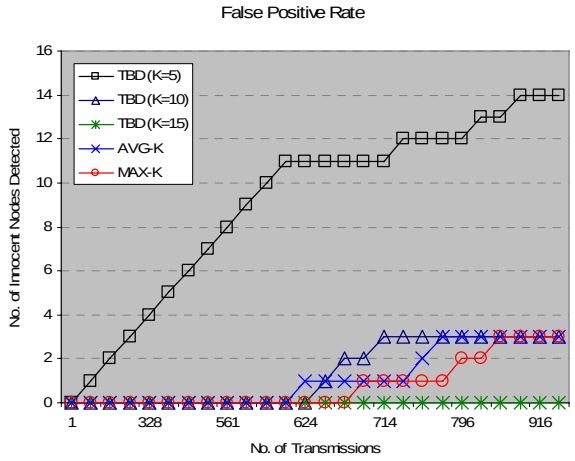
(b)

Fig. 3. (a) Sinkhole Detection Rate and (b) False Positive Rate (ECR = 66, ETR = 50, and 7 sinkholes).

With the TBD (*K*=5) approach, a number of innocent nodes in the network are also detected incorrectly as sinkholes since they are located in bad environment and cannot successfully transmit packets to destination. As shown in Fig. 3(b), the TBD (*K*=5) approach has a high false positive rate compared to the AVG-*K* and MAX-*K* approaches. With no surprise, the AVG-*K* and MAX-*K* approaches could detect the sinkholes while maintaining the low rate of false positives even if the environmental conditions are dynamically changed. Thus, when the environmental turbulence is significant, both AVG-*K* and MAX-*K* approaches provide more accurate sinkhole detection with low false positive rate compared to TBD.



(a)



(b)

Fig. 4. (a) Sinkhole Detection Rate and (b) false positive detection (ECR = 100, ETR = 50, and 7 sinkholes).

6. Conclusions

We present an approach for distinguishing innocent nodes located in poor environment from actual sinkholes. We improve the technique with the mechanism to allow a dynamical adjustment of the *K*-value defined in Thanachai *et al*. 2006. In our improved technique, a dynamic *K*-value is used for separating suspicious behaviors from normal ones so as to reduce false positives. The *K*-value is dynamically adjusted on the basis of the environment where the nodes are located. Our approach allows the nodes to take into consideration the signal strength of their neighbors which is a function of the environmental conditions. If a node is located in bad environment, the node has a higher probability to fail the packet transmission process. With the dynamic *K*-value, the method consequently achieves a high sinkhole detection rate with low false positive rate despite the poor environmental conditions.

7. References

Deng, H.M.; Li, W.; and Agrawal, D.P. 2002. Routing security in wireless ad hoc networks. IEEE Commun. Mag. 40(10): 70-5.

Ramaswamy, S.; Fu, H.; Sreekantaradhya, M.; Dixon, J.; and Nygard, K.E. 2003. Prevention of cooperative black hole attack in wireless ad hoc networks. Proc. Int. Conf. on Wireless Networks (ICDN'03), Las Vegas, NV, USA, 23-26 June, pp. 570-5. CSREA Press, Athens, GA, USA.

Burg, A. 2003. Ad hoc network specific attacks. Paper presented at the Seminar on Ad Hoc Networking: Concept, Applications, and Security, Technische Universität München, Germany, 13 November.

Wu, B.; Chen, J.; Wu, J.; and Cardei, M. 2007. A Survey on Intrustion Detection in Mobile Ad Hoc Networks. In Wireless Network Security, Series: Signals and Communication Technology, Xiao, Y.; Shen, X.; and Du, D.-Z. (eds.), Springer, Berlin, Germany.

Kapil, K.; and Ghosh, R.K. 2005. Cooperative black and gray hole attacks in mobile ad hoc networks.

Zhou, L.; and Haas, Z.T. 1999. Securing ad hoc networks. IEEE Network 13(6): 24-30.

Kurian, J. 2004. Ensuring security in ad hoc networks, T-110.551 Seminar on Internetworking, Helsinki University of Technology, Finland. Available: http://www.tml.tkk.fi/Studies/T-110.551/2004/papers/Kurian.pdf.

Frankel, Y.; Gemmell, P.; MacKenzie, P.; and Yung, M. 1997. Optimal resilience proactive public-key cryptosystems. Proc. 38th Symp. on Foundations of Computer Science (FOCS'97), Miami Beach, FL, USA, 19-22 October, pp. 384-393, IEEE Computer Society, Los Alamitos, CA, USA.

Herzberg, A.; Jakobsson, M.; Jarecki, S.; Krawczyk, H.; and Yung, M. 1997. Proactive public-key and signature systems. Proc. 4th ACM Conf. on Computer Communications Security (CCS'97), Zurich, Switzerland, 1-4 April, pp. 100-110, ACM Press New York, NY, USA.

Asokan, N.; and Ginzboorg, P. 2000. Key agreement in ad hoc networks. Comp. Commun. 23: 1627-37.

Khalili, A.; Katz, J.; and Arbaugh, W.A. 2003. Towards secure key distribution in truly ad-hoc networks. Proc. 2003 Symp. on Applications and the Internet Workshops (SAINT'03 Workshops), 27-31 January, p. 342, IEEE Computer Society, Los Alamitos, CA, USA.

Chen, H.; Ji, Z.; and Hu, M. 2006. A novel security agent scheme for AODV routing protocol based on thread state transition. Asian J. Info. Tech. 5: 54-60.

Marti, S.; Giuli, T.J.; Lai, K.; and Baker, M. 2000. Mitigating routing misbehavior in mobile ad hoc networks. Proc. 6th ACM Int. Conf. on Mobile Computing and Networking, Boston, MA, USA, 6-11 August, pp. 255-265, ACM Press, New York, NY, USA.

Jin, S.; Park, C.; Choi, D.; Chung, K.; and Yoon, H. 2005. Cluster-based trust evaluation scheme in an ad hoc network. ETRI Journal 27(4): 465-8.

Thanachai, T.; Tapanan, Y.; and Punthep, S. 2006. Adaptive sinkhole detection on wireless ad hoc networks. Proc. IEEE Aerospace Conf., Big Sky, Montana, USA, 4-11 March, IEEE, Piscataway, NJ, USA.