Wireless Sensor Network, 2012, 4, 185-190
http://dx.doi.org/10.4236/wsn.2012.48027 Published Online August 2012 (http://www.SciRP.org/journal/wsn)

An Effective Control Report Based Security Countermeasure against the Joint Attacks of False Report Injection Attack and Selective Forwarding Attack

Hyun Woo Lee, Tae Ho Cho
College of Information and Communication Engineering, Sungkyunkwan University, Suwon, Korea
Email: hwoolee@ece.skku.ac.kr, taecho@ece.skku.ac.kr

Received July 2, 2012; revised August 4, 2012; accepted August 13, 2012

ABSTRACT

Sensor networks are vulnerable to many attacks because the sensor networks operate in open environments. It is easy to incur one or more attacks such as a selective forwarding attack, a false report injection attack. It is hard to defend the sensor network from the multiple attacks through existing security methods. Thus, we suggest an energy-efficient security method in order to detect the multiple attacks. This paper presents a security method to detect the false report injection attack and the selective forwarding attack in the sensor network using a new message type. The message type is a filtering message. The filtering message prevents from generating and forwarding false alert messages. We evaluated performance of our proposed method through a simulation in comparison with an application of SEF (statistical en-route filtering scheme) and CHEMAS (Check point-based Multi-hop Acknowledgement Scheme). The simulation results represent that the proposed method is 10% more energy-efficient than the application when the number of false reports is great while retaining the detection performance.

Keywords: False Report Injection Attack; Selective Forwarding Attack; SEF; CHEMAS

1. Introduction

Sensor networks consist of a lot of sensor nodes and one or more base stations (BS). The sensor network is used in environmentally detecting physical changes. Because the sensor network operates in open environments, it is exposed to various attacks [1]. Many researchers have developed a lot of security protocols to defend the various attacks. For example, [2,3] are security protocols for defending sinkhole attacks. [4,5] are the protocols for defending false report injection attacks. [6-8] are the protocols for defending selective forwarding attacks. The security protocols defend only one type of attack. However, multiple attacks occur simultaneously in real environments. A joint attack of a false report injection attack and a selective forwarding attack is one of them. The false report injection attack generates false report related to an event which is actually inexistent and then forwards the false report to a BS. The attack makes sensor nodes waste their energy and cause false alarm. In a selective forwarding attack, an attacker works as a normal node. However, when the attacker receives a report which includes important information, it drops the report. If the two attacks occur in the sensor field, attackers drop reports which contain critical information and forward a false report which is generated by them. In order to prevent the multiple attacks, both a security method such as SEF and the method such as CHEMAS should be executed simultaneously. However, the way to execute the two methods consumes more energy of sensor nodes than that to execute only one method. Besides, unexpected problems may happen to the way to execute the two methods. For example, one compromised node drops an event report which is forwarded by a neighbor node and the other generates the false report and forwards it to the next neighbor node in a sensor network. The false report is detected by a forwarding node in an event report forwarding path. The forwarding node which detects the false report drops the report. However, sensor nodes which send the event report to the next neighbor node cannot know that the report is false and dropped. Thus, if the sensor nodes do not receive the acknowledgement from the next neighbor node within a timeout, they assume that a selective forwarding attack occurs and generates false alert messages. The alert messages are forwarded toward the BS [8]. Owing to false alert messages, the BS collects the false information and points out a node as an attacker incorrectly. In this paper, in order to solve the problem, we propose a method using a new message type which is called a filtering message. When a sensor node detects a false report, the node generates a

filtering message and forwards the message toward the source node. The nodes which receive the filtering messages do not generate alert messages. We estimated a performance of the proposed method through a simulation. The simulation result shows that, compared with the application of SEF and CHEMAS, the proposed method is more energy-efficient while retaining its security level when the rate of false reports is high. The remainder of this paper is organized as follows. Section 2 discusses SEF and CHEMAS, and the motivation. Section 3 introduces the design of our method. Section 4 discusses the simulation for the proposed method. Section 5 concludes the proposed method and outlines future work.

2. Background

2.1. SEF

SEF is a security protocol that each forwarding node detects and drops false reports early in a wireless sensor network. SEF is composed of a key assignment, report generation, en-route filtering and base station verification. **Figure 1** shows the key assignment and the report generation phase. **Figure 1(a)** indicates the key assignment phase. **Figures 1(b)** and **(c)** indicate a report generation phase. In SEF, A BS contains a global key pool. The global key pool is divided into some partitions. Each partition includes several keys. The key assignment is executed before nodes are deployed in a sensor field. Each node stores several keys randomly in the global key pool. After the key assignment, the sensor nodes are deployed. If an event occurs in the sensor field, some nodes which detect the event elect a CoS (center of stimulus) node in the report generation (**Figure 1(b)**). The nodes forward their MACs (message authentication codes) and the event information to the CoS node. The CoS node generates an event report which contains the MACs and the event information. The CoS node also sends the event report to next a forwarding node (**Figure 1(c)**). After the report generation, phase, when a forwarding node receives the event report, the node verifies the report in the en-route filtering. If the report is false, the node drops the one. In order to verify the event report, each forwarding node confirms indices of partitions of the event report. If there is a corresponding index to the index that the node contains, the forwarding node generates a MAC using its key which has the corresponding index. Then the node compares its MAC with a MAC of the key index in the event report. If the two MACs are the same, the node forwards the event report to the next forwarding node. However, if the two MACs are not the same, the node drops the one. In the base station verification, the BS contains all keys which can verify event reports. Thus, BS drops all false reports which are not filtered in en-route filtering phase.

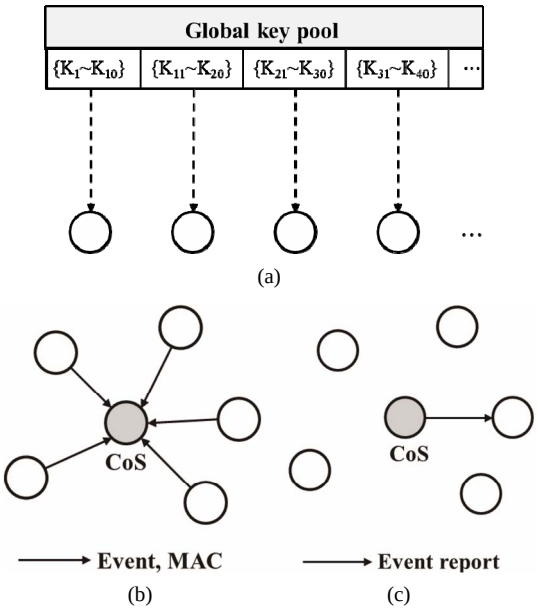
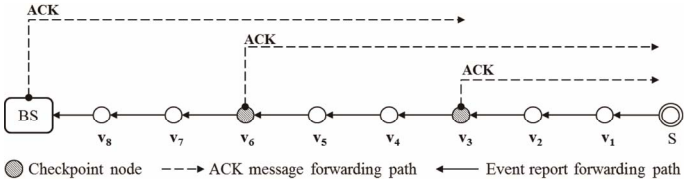


Figure 1. Key assignment and report generation phases.

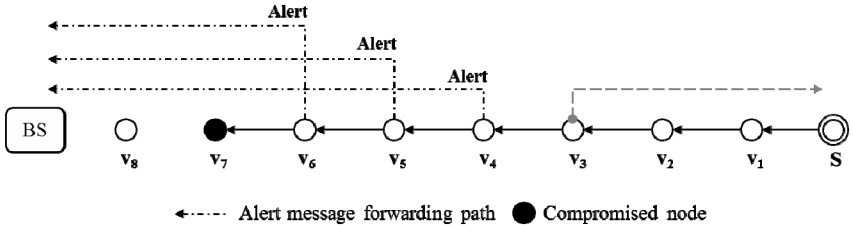
2.2. CHEMAS

When a selective forwarding attack occurs in a wireless sensor network, in CHEMAS, forwarding nodes detect the attack using acknowledgement themselves. Two message types are used to detect the selective forwarding attack. The two message types are an ack message and an alert message. The ack messages are used to confirm forwarding the event report. The alert messages are used to forward information of a node which is suspected as attackers to the BS. **Figure 2** shows examples of using the two message types in CHEMAS.

Sensor nodes which are selected as checkpoint nodes among forwarding nodes which receive the event report forward ack messages to a neighbor node through the event report forwarding path in an opposite direction so as to detect selective forwarding attacks. For example, the event report is forwarded from the source node S to the BS. The forwarding nodes which receives the event report, confirm whether each node is a checkpoint node or not through a checkpoint selection [8]. After the confirmation, if the node is the checkpoint node, the node generates an ack message and forwards it to an event report forwarding path in an opposite direction. After sending the event report, each forwarding node waits for receiving ack messages from its downstream nodes. If the forwarding node does not receive the ack message during fixed in time due to a selective forwarding attack, the node generates an alert message and forwards it to the BS. In **Figure 2(b)**, when a compromised node v_7 drops an event report, forwarding nodes which send the event report v_4, v_5 and v_6 cannot receive ack messages. v_4, v_5 and v_6 generate alert messages and forward them to the BS. Each alert message contains a node's ID which



(a) Ack message generation and forwarding.



(b) Event report drop and alert message generation and forwarding.

Figure 2. Examples of use of an ack message an alert message.

is suspected as a compromised node which drops the event report. The suspect node's ID is an immediate downstream node's ID of the node which generates alert messages. In **Figure 2(b)**, v_6 points out v_7 as a suspect node, v_5 indicates v_6 and v_4 points out v_5. BS collects and analyzes the alert messages and then selects a compromised node. The selected node is excluded in the next routing.

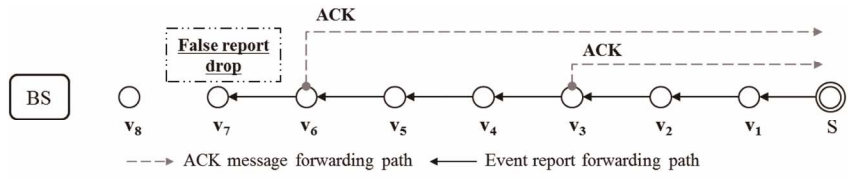
2.3. Motivation

When a false report injection attack occurs in a sensor network, if SEF and CHEMAS are executed simultaneously, there is a problem. **Figure 3** shows the problem when both SEF and CHEMAS are executed. In **Figure 3**, sensor nodes forward an event report to downstream nodes. The nodes should receive two ack messages. When a compromised node forwards a false report to its neighbor node, the node which received the false report verifies and drops the report. In **Figure 3(a)**, v_7 drops the false report. However, v_4, v_5 and v_6 do not know whether the event report was dropped or not. Thus, although there is not a selective forwarding attack, they assume that the attack occurs. They generate and forward alert messages to a BS in **Figure 3(b)**. Likewise, sensor nodes consume their energy by forwarding the false alert messages. They also forward false information to the BS. In proposed method, in order to decrease energy of sensor nodes which are used to forwarding false alert messages, a filtering message is added. The message decreases generation of the false alert messages.

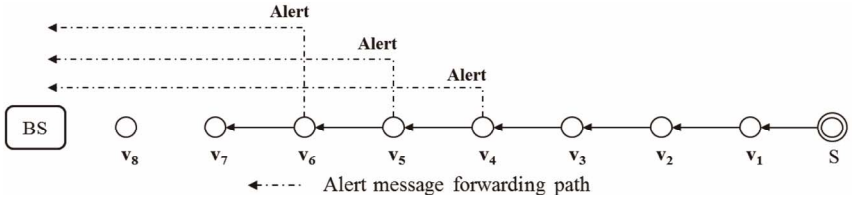
3. Proposed Method

3.1. Assumption

We made the third assumptions in applying the proposed method. First, we assume that selective forwarding attacks often occur in similar areas; Second, we assume that event reports contain its unique ID; Third, we assume that μTESLA [9] has been implemented in each sensor node [8].



(a) False report detection and drop.



(b) False detection of selective forwarding attack and alert message generation and forwarding.

Figure 3. A problem when both SEF and CHEMAS are executed.

3.2. Filtering Message Scheme

The filtering message scheme of the proposed method helps distinguish the false report drop and the selective forwarding attack in the report forwarding phase. **Figure 4** shows the operation process of a sensor node when the node receives an event report.

The node which receives the event report checks whether the node is a checkpoint node or not by using the checkpoint selection function [8]. If the node becomes the checkpoint node, the node generates an ack message and forwards the message to upstream nodes. After the confirmation, the node verifies the event report through MAC comparison. When the event report is normal, the report is forwarded to downstream nodes. However, if the report is false, the node which verified the false report generates a filtering message and forwards the message to upstream nodes. **Figure 5** indicates a filtering message forwarding process. When a sensor node which detects a false report injection attack drops the false report, the node generates a filtering message. The filtering message is forwarded to its upstream nodes. In **Figure 5**, v_7 drops the false report and sends a filtering message to the source node S. The upstream node which receives the filtering message does not wait for the ack messages until the node receives a new event report. The node also does not make a false alert message. **Figure 6** shows a filtering message format. As shown in **Figure 6**, a filtering message is composed of Message_header, Event_report_id, and Node_id. Message_header refers to the header of a filtering message. Event_report_id refers to an event report's id which is dropped by a forwarding node. Node_id refers to a node's id which generates a filtering message. The filtering message decreases communication costs of false alert messages. **Table 1** shows the number of communication of sensor nodes in terms of **Figures 3(a)** and **5**. **Figure 3(a)** is the case when a filtering message is not used in a sensor network. **Figure 5** is a case when filtering message is used.

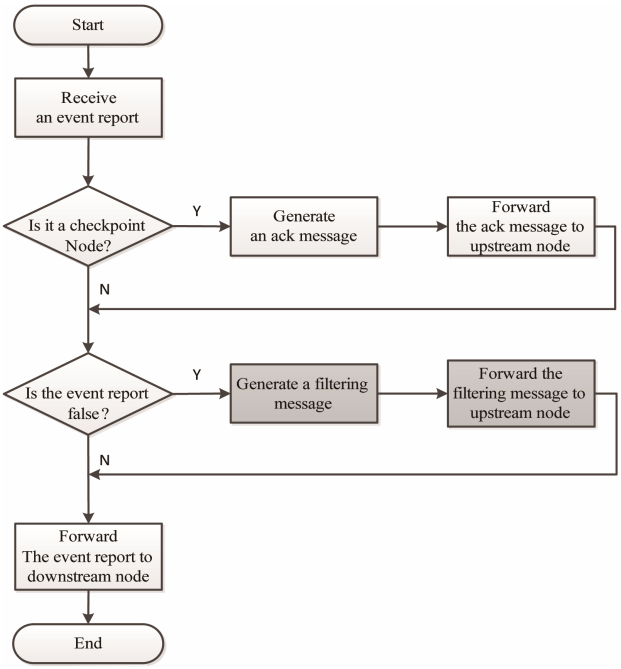


Figure 4. Operation process of sensor node which receives an event report.

Table 1. The number of communication with/without filtering message.

	v_4	v_5	v_6	v_7	v_8	SUM
The number of transmitted messages						
Figure 3(a)	0	2	3	3	3	11
Figure 5	0	1	1	1	0	4
The number of received messages						
Figure 3(a)	0	1	2	3	3	9
Figure 5	1	1	1	0	0	3

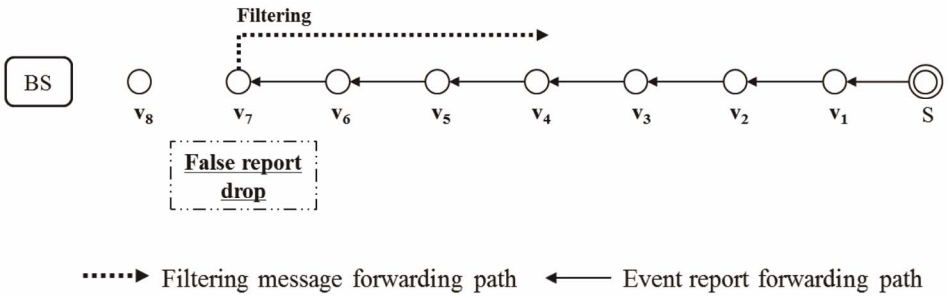


Figure 5. False report detection and filtering message generation and filtering.

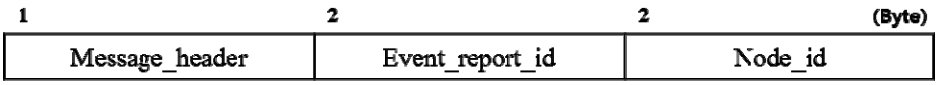


Figure 6. Filtering message format.

In **Table 1**, the number of sent messages in **Figure 5** is lower than the case of **Figure 3(a)**. Likewise, we expect that when a false report injection attack and selective forwarding attacks occur, the proposed method is more energy-efficient than the case when both SEF and CHEMAS are executed. The method also makes the false alert messages be forwarded to the BS. We check the performance of the method through simulation.

4. Simulation

In this section, we evaluated the performance of proposed method through simulation in terms of security and energy consumption. This simulation scenario uses a sensor field with size of 100 × 100 m^2 where 600 nodes are distributed. In the simulation, a total of 100 event reports are generated by the source nodes. When a report or message is forwarded, each node consumes energy such as 16.25 μJ, 12.5 μJ to transmit and receive a byte [4]. The node also consumes energy 75 μJ to verify the report or message [4]. The size of an event report is 24 bytes [4]. The sizes of an ack message and an alert message are 11 bytes and 12 bytes, respectively [8]. The size of a filtering message is 5 bytes. **Figure 7** shows the detection probabilities under the number of compromised nodes in a sensor network in order to evaluate security in terms of selective forwarding attacks.

Figure 7 indicates that when a selective forwarding attack occurs, both the application of SEF and CHEMAS and proposed method detection probabilities are 89%. The detection probability is calculated by the rate of detected selective attacks by the methods under the total number of selective forwarding attacks in the sensor network. The proposed method focuses on energy consumption when the false report injection attacks occur. Thus, when selective forwarding attacks occur, the security of proposed method is the same as the one of the application. **Figure 8** shows the number of undetected false reports under the rate of false reports to calculate security in terms of false report injection attacks.

In **Figure 8**, the rate of false reports is estimated by the number of false reports divided by the total number of event reports which are generated a sensor field. The number of undetected false reports is the number of the reports which survived in the report forwarding phase and arrived at BS. An average number of the number of false reports in an application of SEF and CHEMAS is 0.5 and one of the number of the reports in the proposed method is 0.53. The security of the two methods is similar. **Figure 9** shows energy consumption of sensor nodes under the rate of false reports when false report injection attacks and selective forwarding attacks occur in the sensor field.

In **Figure 9**, energy consumption is calculated by the sum of communication energy and verification energy of the nodes. When the rate of false reports was less than 30%, subtraction of the two methods was less than 5% in **Figure 9**. However, when the rate of false reports was 50%, the subtraction was 10.4%. The rate of false reports was greater, the subtraction was greater. Because when the rate of false reports is great, the incremented number of false alert messages in the application of SEF and CHEMAS is far greater than the increased number of filtering messages in the proposed method. Thus, the proposed method consumed less energy than the application. We found out that when the rate of false reports is great, the proposed method becomes energy efficient and keeps the security which is similar to the application in the sensor network through simulation.

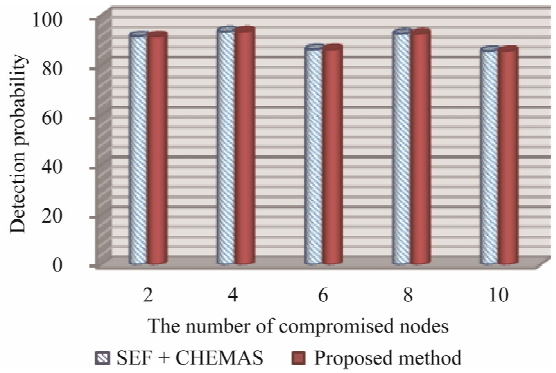


Figure 7. Detection probability versus the number of compromised nodes.

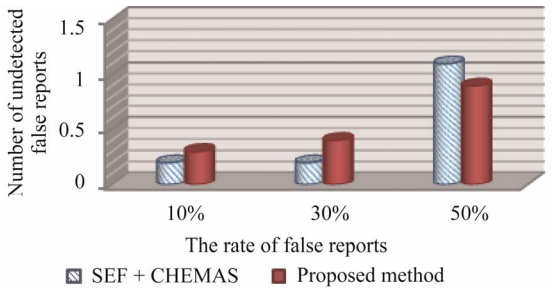


Figure 8. The number of undetected false reports versus the rate of false reports.

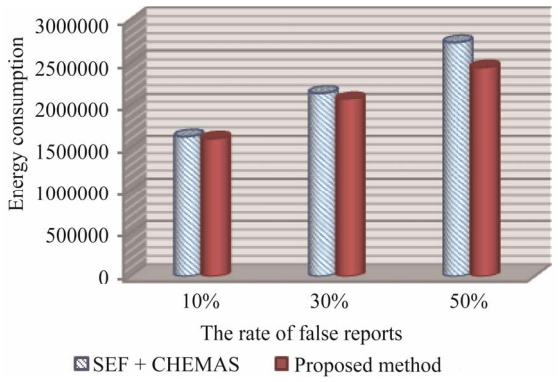


Figure 9. Energy consumption versus the rate of false reports.

5. Conclusion and Future Work

Wireless sensor networks are operated in open and hostile environments. The sensor networks are in the face of danger in terms of security. Thus, there is a high probability of multiple attacks in the networks. When the multiple attacks happen at the same time in the sensor network, it is difficult for the existing security methods to prevent the multiple attacks such as the false report injection attack and the selective forwarding attack. Besides, when the security methods are simultaneously used to detect the multiple attacks, sensor nodes consume unnecessary energy. For a successful operation, it is necessary to avoid unnecessary energy consumption. In this paper, we proposed an energy-efficient method using a filtering message which is a new message type to detect the multiple attacks such as the false report injection attack and the selective forwarding attack. We expected to present a better energy efficient method than the existing methods. Then, we found out energy efficiency of the proposed method through simulation. We have studied the multiple attacks which are the false report injection attack and the selective forwarding attack. As our future work, we are going to study on a security method to detect other multiple attacks.

6. Acknowledgements

This research was supported by Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Education, Science and Technology (No. 2012-0002475).

REFERENCES

[1] I. F. Akyildiz, S. Weilian, Y. Sankarasubramaniam and E. Cayirci, "A Survey on Sensor Networks," *IEEE of Communications Magazine*, Vol. 40, No. 8, 2002, pp. 102-114. doi:10.1109/MCOM.2002.1024422

[2] T. F. Smith and M. S. Waterman, "Identification of Common Molecular Subsequences," *Journal of Molecular Biology*, Vol. 147, No. 1, 1981, pp. 195-197. doi:10.1016/0022-2836(81)90087-5

[3] E. C. H. Ngai, J. Liu and M. R. Lyu, "An Efficient Intruder Detection Algorithm against Sinkhole Attacks in Wireless Sensor Networks," *Computer Communications*, Vol. 30, No. 11-12, 2007, pp. 2353-2364. doi:10.1016/j.comcom.2007.04.025

[4] F. Ye, H. Luo and S. W. Lu, "Statistical En-Route Filtering of Injected False Data in Sensor Networks," *Twenty-Third Annual Joint Conference of the IEEE Computer and Communications Societies*, Vol. 4, 2004, pp. 2446-2457.

[5] Z. Yu and Y. Guan, "A Dynamic En-Route Filtering Scheme for Data Reporting in Wireless Sensor Networks," *IEEE/ACM Transactions on Networking*, Vol. 18, No. 1, 2010, pp. 150-163. doi:10.1109/TNET.2009.2026901

[6] B. Xiao and B. Yu, "Detecting Selective Forwarding Attacks in Wireless Sensor Networks," 20*th International, Parallel and Distributed Processing Symposium, IPDPS* 2006, 25-29 April 2006, pp. 25-29.

[7] H. J. Deng, X. M. Sun, B. W. Wang and Y. F. Cao, "Selective Forwarding Attack Detection Using Watermark in WSNs," *ISECS International Colloquium on Computing, Communication, Control*, and *Management, CCCM* 2009, Sanya, 8-9 August 2009, Vol. 3, pp. 109-113. doi:10.1109/CCCM.2009.5268016

[8] B. Xiao, B. Yu and C. S. Gao, "Chemas: Identify Suspect Nodes in Selective Forwarding Attacks," *Journal of Parallel and Distributed Computing*, Vol. 67, No. 11, 2007, pp. 1218-1230. doi:10.1016/j.jpdc.2007.04.014

[9] R. Szewczyk, A. Perrig, J. D. Tyger, V. Wen and D. E. Culler, "Spins: Security Protocols for Sensor Networks," *Proceedings of ACM MobiHoc*, Annapolis, June 2003, pp. 177-188.

