IOSR Journal of Electronics & Communication Engineering (IOSR-JECE)
ISSN : 2278-2834, ISBN : 2278-8735, PP : 55-62
www.iosrjournals.org

Sensing methods for Intrusion Detection in Homogeneous and Heterogeneous Wireless Sensor Networks

S.R. Shetake[1], S.S.Sannakki[2]
[1]*Department of Computer Science and Engg.,*
Gogte Institute of Technology,Belgaum

Abstract: *Intrusion detection in Wireless Sensor Network (WSN) is of practical interest in many applications such as detecting an intruder in a battlefield. The intrusion detection is defined as a mechanism for a WSN to detect the existence of inappropriate, incorrect, or anomalous moving attackers. In this paper, we consider this issue according to heterogeneous WSN models. Furthermore, we consider two sensing detection models: single-sensing detection and multiple-sensing detection. simulation results show the advantage of multiple sensor in heterogeneous WSNs.Wireless sensor networks are tremendously being used to perform various monitoring tasks such as search,rescue,disaster*
Relief,target tracking and number of tasks in smart environments.WSN in three dimensional space is common in different application ares such as space monitoring,cave monitoring under water eco system and so on.

I.Introduction:

A Wireless Sensor Network (WSN) is a collection of spatially deployed wireless sensors by which to monitor various changes of environmental conditions (e.g., forest fire, air pollutant concentration, and object moving) in a collaborative manner without relying on any underlying infrastructure support .Recently, a number of research efforts have been made to develop sensor hardware and network architectures in order to effectively deploy WSNs for a variety of applications. Due to a wide diversity of WSN application requirements, however, a general-purpose WSN design cannot fulfill the needs of all applications. Many network parameters such as sensing range, transmission range, and node density have to be carefully considered at the network design stage, according to specific applications. To achieve this, it is critical to capture the impacts of network parameters on network performance with respect to application specifications. Intrusion detection (i.e., object tracking) in a WSN can be regarded as a monitoring system for detecting the intruder that is invading the network domain.

The intrusion detection application concerns how fast the intruder can be detected by the WSN. If sensors are deployed with a high density so that the union of all sensing ranges covers the entire network area, the intruder can be immediately detected once it approaches the network area.

Intrusion detection (i.e., object tracking) in a WSN can be regarded as a monitoring system for detecting the intruder that is invading the network domain. Fig. 1gives an example that sensors are deployed in a square area (A=L×L) for detecting the presence of a moving intruder. Note that in Fig. 1, as well as in Figs. 3 and 4, the illustration of sensors and an intruder is based on a slide. The intrusion detection application concerns how fast the intruder can be detected by the WSN. If sensors are deployed with a high density so that the union of all sensing ranges covers the entire network area, intruder can be immediately detected once it approaches the network area. However, such a high-density deployment policy increases the network investment and may be even unaffordable for a large area. In fact, it is not necessary to deploy so many sensors to cover the entire WSN area in many applications [3], since a network with small and scattered void areas will also be able to detect a moving intruder within a certain intrusion distance In this case, the application can specify a required intrusion distance within which the intruder should be detected. As shown in Fig. 1,the intrusion distance is referred as D and defined as the distance between the point the intruder enters the WSN, and the point the intruder is detected by the WSN system. This distance is of central interest to a WSN used for
intrusion detection.

We derive the expected intrusion distance and evaluate the detection probability in different application scenarios. Given a maximal allowable intrusion distance Dmax = € we theoretically capture the impact on the detection probability in terms of different network parameters, including node density, sensing range, and transmission range. For example, given an expected detection distance E(D), we can derive the node density with respect to sensors' sensing range, thereby knowing the total number of sensors required for WSN deployment

In a WSN, there are **t**wo ways to detect an object(i.e., an intruder): single-sensing detection and multiple-sensing detection. In the single-sensing detection, the intruder can be successfully detected by a single sensor. On the contrary, in the multiple-sensing detection, the intruder can only be detected by multiple collaborating

sensors [4]. In some applications, the sensed information provided by a single sensor might be inadequate for recognizing the intruder. It is because individual sensors can only sense a portion of the intruder. For example, the location of an

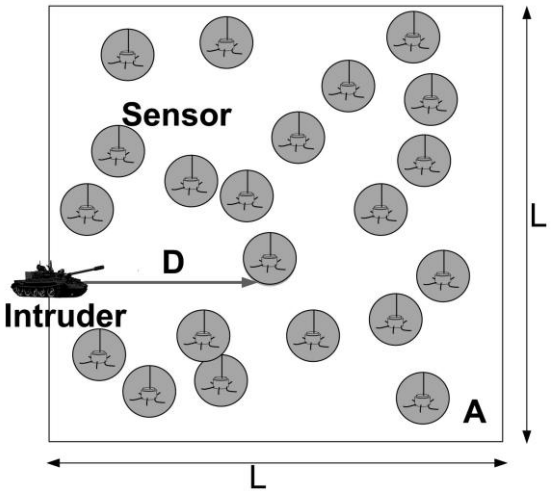

Fig. 1. Intrusion detection in a WSN.

intruder can only be determined from at least three sensors' sensing data [5], [6], [7], [8]. In view of this, we analyze the intrusion detection problem under two application scenarios: single-sensing detection and multiple-sensing detection. According to the capability of sensors, we consider two network types: homogeneous and heterogeneous WSNs [9]. We define the sensor capability in terms of the
sensing range and the transmission range. In a heterogeneous WSN[10], [11], [12] some sensors have a larger sensing range and more power to achieve a longer transmission range. In this paper, we show that the heterogeneous WSN increases the detection probability for a given intrusion detection distance. On the other hand, a heterogeneous WSN poses the challenge of network connectivity due to asymmetric wireless link. The high-capability sensors have a longer transmission range while low capability sensors have a shorter transmission range. Due to this, the packet sent by a high-capability sensor may reach the low-capability sensor, while the low capability sensor may not be able to send packets to the corresponding high-capability sensor[13]. This motivates us to analyze the network connectivity
in this paper. Furthermore, in a heterogeneous WSN, high capability sensors usually undertake more important tasks(i.e., broadcasting power management information or synchronization information to all the sensors in the network),it is also desirable to define and examine the broadcast reach ability from high-capability sensors. The network connectivity and broadcast reach ability are important conditions
to ensure the detection probability in WSNs. They
are formally defined and analyzed in this paper. To the best of our knowledge, our effect is the first to address this issue in a heterogeneous WSN.

II.1ntrusion detection

An **Intrusion detection system** (**IDS**) is software and/or hardware designed to detect unwanted attempts at accessing, manipulating, and/or disabling of computer mainly through a network, such as the Internet. These attempts may take the form of attacks, as examples, by crackers,, malwarer and/or disgruntled employees. IDS cannot directly detect attacks within properly encrypted traffic.
An intrusion detection system is used to detect several types of malicious behaviors that can compromise the security and trust of a computer system. This includes network attacks against vulnerable services, data driven attacks on applications, host based attacks such as privilege escalation, unauthorized logins and access to sensitive files, and viruses
IDS can be composed of several components: **Sensors** which generate security events, a **Console** to monitor events and alerts and control the sensors, and a central **Engine** that records events logged by the sensors in a database and uses a system of rules to generate alerts from security events received. There are several ways to categorize an IDS depending on the type and location of the sensors and the methodology used by the engine to generate alerts. In many simple IDS implementations all three components are combined in a single device or appliance.

2.1 Intrusion detection model & definations

intrusion detection model includes a network model,a detection model, and an intrusion strategy model.The network model specifies the WSN environment. The detection model defines how the intruder can be detected and the intrusion strategy illustrates the moving policy of the intruder.

2. 2 Network Model

consider a WSN in a two-dimensional (2D) plane with N sensors, denoted by a set $N(n1, n2 \ldots n_N)$, where n_i is the **i**th sensor. These sensors are uniformly and indepen- dently deployed in a square area A =L×L Such a random deployment results in a 2D Poisson point distribution of sensors. All sensors are static once the WSN has been deployed. In particular, we consider two WSN types: homogeneous and heterogeneous WSNs. In a homogeneous WSN, each sensor has the same sensing radius of r_S, and the transmission range of r_X. A sensor can only sense the intruder within its sensing coverage area that is a disk with radius r_S centered at the sensor. Denote the node density of the homogeneous WSN as λ
then focus on a heterogeneous WSN with two types of sensors, as shown in Fig. 2:

- Type I sensor that has a larger sensing range r_{S1}, as well as a longer transmission range r_{X1}, and
- Type II sensor that has a smaller sensing range r_{S2}, as well as a shorter transmission range r_{X2}.

The densities of Type I and Type II sensors are represented as λ_1 and λ_2, respectively.

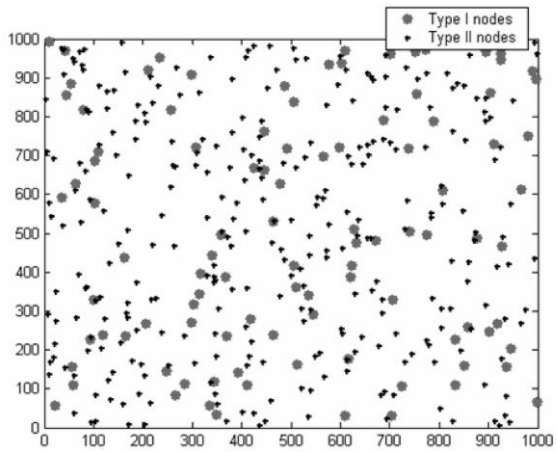

Fig. 2. Heterogeneous WSN deployment.

WSN, where both Type I and Type II sensors follow the 2D Poisson point distribution. In a homogeneous or heterogeneous WSN, a point is said to be covered by a sensor if it is located in the sensing range of any sensor(s). The WSN is thus divided into two regions, the covered region, which is the union of all sensor coverage disks, and the uncovered region, which is the complement of the covered region within the area of interest A. In our network model, the intruder does not know the sensing coverage map of the WSN.

There are two detection models in terms of how many
sensors are required to recognize an intruder: single sensing detection model and multiple-sensing detection model. It is said that the intruder is detected *under the single-sensing detection model if the* intruder can be identified by using the sensing knowledge from one single sensor.On the contrary, in the multiple-sensing detection model, the intruder can only be identified by using cooperative knowledge from at least k sensors (k is defined by specific application requirements). For simplicity of expression, multiple sensing and k-sensing are interchangeable in the following discussion:

In order to evaluate the quality of intrusion detection in
WSNs, we define three metrics as follows:

a) **Intrusion distance**

The intrusion distance, denoted by D, is the distance that the intruder travels before it is detected by a WSN for the first time. Specifically, it is the distance between the point where the intruder enters the WSN and the point where the intruder gets detected by any sensor(s). Following the definition of intrusion distance, the Maximal Intrusion Distance (denoted by ε, $\varepsilon > 0$)
is the maximal distance allowable for the intruder
to move before it is detected by the WSN.

b) Detection probability:

The detection probability is defined as the probability that an intruder is detected within a certain intrusion distance (e.g.,Maximal Intrusion Distance ε).

c) Average intrusion distance.

The average intrusion distance is defined as the expected distance that the intruder travels before it is detected by the WSN for the first time.

III. Intrusion detection in homogeneous

Wireless sensor network

we see the analysis of intrusion detection in a homogeneous WSN. We derive the detection probability for single-sensing detection and k-sensin detection.

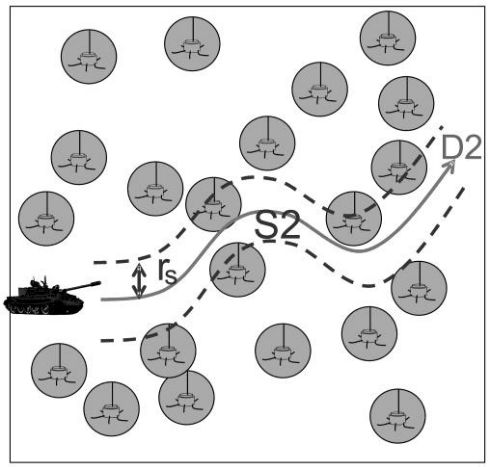

Fig. 3. Intrusion strategy 2.

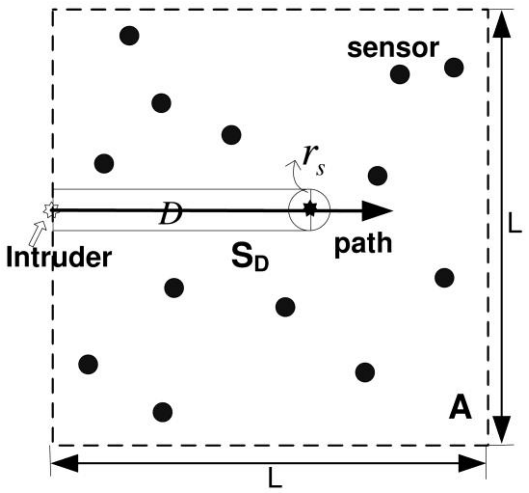

Fig. 4. The intruder starts from the boundary of the WSN.

3.1 Single-Sensing Detection

In the single-sensing detection model, the intruder can be recognized once it moves into the sensing coverage disk of any sensor(s). According to the intrusion strategy, the intruder may access the network domain from any point of the network boundary or a random point in the network domain. When the intruder starts from a point of the network boundary, as shown in Fig 4, given an

intrusion distance D >0, the corresponding intrusion detection area SD is almost an oblong area. This area includes a rectangular area with length D and width 2rs and a half disk with radius rs attached to it. It has

$S_D = 2 * D*rs+JIr2/2$

According to the definition of single-sensing detection, the intruder is detected if and only if there exists at least one sensor within this area SD. Otherwise, the intruder is not detected. Similarly, when the intruder starts from a random point in the network domain, the corresponding intrusion detection area is

$S_D = 2 * D*rs+Jr^2$

in Fig. 5. In the following analysis, we focus on the case that the intruder starts from the boundary of the network domain.

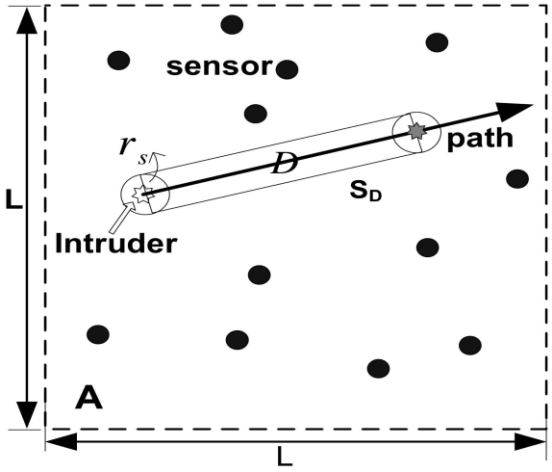

Fig. 5. The intruder starts form a random point in the WSN.

3.2 K-Sensing Detection

In the k-sensing detection model, an intruder has to be sensed by at least k sensors for intrusion detection in a WSN. The number of required sensors depends on specific applications.

For example, at least three sensors' sensing information is required to determine the location of the intruder.

IV.Intrusion detection in a heterogeneous Wireless sensor network

In a heterogeneous WSN, as defined in Section 3.1, consider two types of sensors: Type I and Type II with the node density of λ 1 and λ 2, respectively. A Type I sensor has the sensing range rs1, and the sensing coverage is a disk of area $S1= Jr^2_{s1}$

. A Type II sensor has the sensing coverage of

$S2 = Jr^2_{s2}$ with the sensing range rs2. Without

loss of generality, we can assume that rs1 > rs2 in our

network model. In a heterogeneous WSN, any point in the network domain is said to be covered if the point is under the sensing range of any sensor (Type I, Type II, or both).

In this section, we present the analysis of intrusion

detection probability of a heterogeneous WSN in single sensing detection and multiple-sensing detection models.

4.1 Single-Sensing Detection

We denote the intrusion distance by Dh in the given heterogeneous WSN. Again, an intruder may be detected by the WSN once it approaches the network boundary, and the corresponding intrusion distance is Dh = 0.

According to the single-sensing detection model,

the intruder is detected if and only if one of the following conditions is satisfied:

. The intruder enters into the sensing coverage area
of any Type I sensor(s).

. The intruder enters into the sensing coverage area
of any Type II sensor(s).

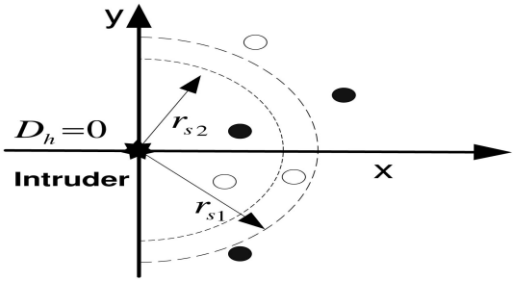

Fig.6 Intrusion detection at the start point (Dh =0)

4.2 K-Sensing in a Heterogeneous WSN

In the k-sensing detection model of a heterogeneous WSN with two types of sensors, at least k sensors are required to detect an intruder. These k sensors can be any combination of Type I and Type II sensors. For instance, if three sensors are required to detect an intruder for a specific application, the intruder can be detected by any of the following sensor combinations:

1. three Type I sensors,
2. three Type II sensors,
3. one Type I sensor and two Type II sensors,
4. two Type I sensors and one Type II sensor

V. Network connectivity and broadcast Reachability in a heterogeneous Wireless sensor network

Based on our network model, Theorems 1-12 statistically characterize the intrusion detection probability in terms of the intrusion distance, the node density, the sensing range, and the node heterogeneity. Given a maximal allowable intrusion distance, a predefined detection probability, and the sensor capability (i.e., sensing range), the network planner can calculate the required node density .The network planner knows the number and type of sensors that have to be deployed in the WSN.

However, detecting the intruder is the first step in intrusion detection. To operate successfully, a WSN must provide satisfactory connectivity so that sensors can communicate for data collaboration and reporting to the administrative center (i.e., base station). The sensing data may have to be reported to the base station, which may be in any location of the network If the network connectivity is not assured, it is meaningless even the sensor(s) detect the presence of the intruder is that in a homogeneous WSN, if the transmission range is equal to or higher than twice of the sensing range, a given coverage probability guarantees a connectivity probability.

In this manner, when the coverage is satisfied in the homogeneous WSN, the network connectivity is also statistically guaranteed so that it allows two sensors to communicate with each other. However, in a heterogeneous WSN, the deployment of sensors with different capability complicates the network operation with the asymmetric links. Specifically, a sensor with longer transmission range (i.e., Type I sensor) might reach some sensors with shorter transmission range (i.e., Type II sensors), while the Type II sensors may not be able to reach the Type I sensor. The network connectivity has to be reconsidered.

In heterogeneous WSN, sensors mainly use a broadcast paradigm for communication [12] and high-capacity sensors usually undertake more important tasks (i.e., for broadcasting power management information or synchronization information to all the sensors). This motivates us to examine two fundamental characteristics of a heterogeneous WSN.

The definitions are listed below:

Network connectivity. The probability that a packet broadcasted from any sensor (either Type I or Type II sensor) can reach all the other sensors in the network.

Broadcast reachability. The probability that a packet broadcasted from any Type I sensor can reach all the other sensors in the network.

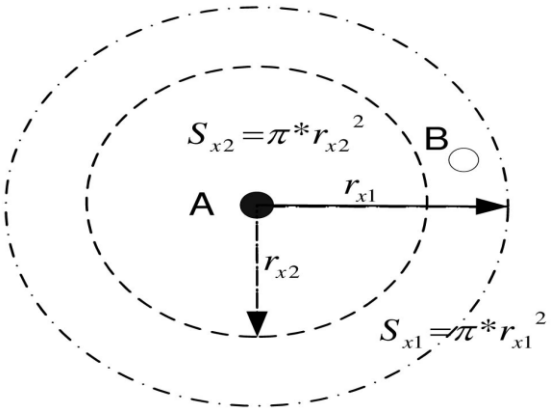

Fig. 7.Transmission range in heterogeneous case.

Given node densities and the transmission ranges of different sensors deployed in a WSN, we can reachability. On the other hand, if the required network connectivity (or broadcast reachability) is specified, we can compute the required transmission ranges in terms of node density. Thus, the minimal transmission power can be obtained for the purpose of power efficiency. In, Bettstetter has proved the following lemma on the network connectivity of WSNs using sensors with different transmission ranges.

VI. Simulation and Verification:-

A simulation-based verification of our
analytical results in both homogeneous and heterogeneous WSNs. The simulation is carried out for single-sensing and k-sensing detection models. The analytical and simulation results are compared by varying the sensing range, transmission range, node density, and node availability. In the simulation, sensors are deployed in accordance with a uniform distribution in a squared network domain. The intruder moves into the network domain from a randomly selected point on the network boundary. Monte-Carlo simulation is performed, and each data point shown in the following figures is the average of 500 simulation results.

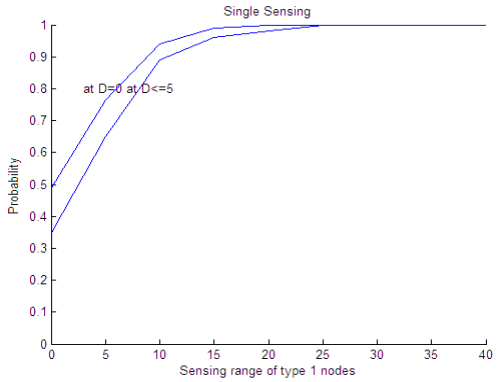

Fig. 8 Single sensing probability analysis

Above Fig. shows Single-Sensing detection probability and Multi sensing- detection probability. It is evident that the single sensing detection probability is higher than that of multi sensing- detection probability .This is because the multi sensing detection imposes a more stricter requirement on detecting the intruder. It also demonstrates that the detection probability in single sensing detection approaches the value 1 when the sensing range of type 1 increases to a certain threshold. For example, in the single-sensing detection, the intruder can be detected with probability 1 if the sensing range exceeds 25. In order to get the result we fixed the type 2 sensors as 300 and its sensing range is set as 10. Total 200 type 1 sensors are deployed uniformly and its sensing range is varied from 0 to 40. It shows that the sensing range significantly impacts the detection probability of a heterogeneous WSN

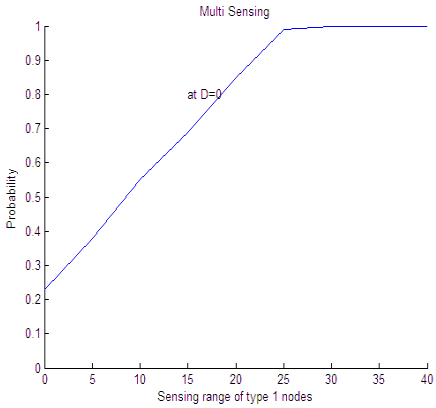

Fig. 9 Multisensing probability analysis

Fig. Demonstrates multi sensing detection probability in the same environment as that used for single sensing

Conclusions:-

This paper analyzes the intrusion detection problem by characterizing intrusion detection probability with respect to the intrusion distance and the network parameters (i.e., node density, sensing range, and

transmission range).The analytical model for intrusion detection allows us to analytically formulate intrusion detection probability within a certain intrusion distance under various application scenarios.

REFERENCES

[1] D.P. Agrawal and Q.-A. Zeng, Introduction to Wireless and Mobile Systems. Brooks/Cole Publishing, Aug. 2003.

[2] B. Liu and D. Towsley, "Coverage of Sensor Networks: Fundamental Limits," Proc. Third IEEE Int'l Conf. Mobile Ad Hoc and Sensor Systems (MASS), Oct. 2004.

[3] S. Ren, Q. Li, H. Wang, X. Chen, and X. Zhang, "Design and Analysis of Sensing Scheduling Algorithms under Partial Coverage for Object Detection in Sensor Networks," IEEE
Trans. Parallel and Distributed Systems, vol. 18, no. 3, pp. 334-350, Mar. 2007.

[4] S. Banerjee, C. Grosan, A. Abraham, and P. Mahanti, "Intrusion Detection on Sensor Networks Using Emotional Ants," Int'l J. Applied Science and Computations, vol. 12, no. 3, pp. 152-173, 2005.

[5] S. Capkun, M. Hamdi, and J. Hubaux, "GPS-Free Positioning in Mobile Ad-Hoc Networks," Proc. 34th Ann. Hawaii Int'l Conf.System Sciences, Jan. 2001.

[6] B. Liu, P. Brass, O. Dousse, P. Nain, and D. Towsley, "Mobility Improves Coverage of Sensor Networks," Proc. Sixth ACM Int'l Symp. Mobile Ad Hoc Networking and Computing (MobiHoc '05), pp. 300-308, 2005.

[7] X. Wang, Y. Yoo, Y. Wang, and D.P. Agrawal, "Impact of Node Density and Sensing Range on Intrusion Detection in Wireless Sensor Networks," Proc. 15th Int'l Conf. Computer Comm.and Networks (ICCCN '06), Oct. 2006.