Indian Journal of Science and Technology, Vol 9(28), DOI: 10.17485/ijst/2016/v9i28/95338, July 2016
ISSN (Print) : 0974-6846
ISSN (Online) : 0974-5645

To Propose a Novel Technique for Detection and Isolation of Misdirection Attack in Wireless Sensor Network

Meenu Saini*, Rajan Kumar and Jasleen kaur

Department of Computer Science and Engineering, Chandigarh University, Mohali - 140413, Punjab, India;
sainimeenu229@gmail.com, Cucse.rajan@gmail.com, jasleenkaur2136@gmail.com

Abstract

Objectives: To implement misdirection attack and analyze network performance of LEACH protocol; to propose node localization based technique to detect and isolate misdirection attack; to implement existing and the proposed techniques and compare the consequences in terms of throughput, delay and energy consumption. **Method**: In this manner, a novel procedure has been proposed for the detection and isolation of the misdirection assault in Wireless Sensor Networks. The proposed technique is based on node localization, in which delay per hop is counted and the node which is increasing delay maximum times which can be detected as a malicious node. **Findings:** The simulation of the planned algorithm is performed in NS2 by taking area of 800*800 meters and the numbers of nodes are 20. It has been analyzed that network throughput is to raise and the delay and energy utilization of the sensor nodes lessened.

Keywords: Assaults in Wireless Sensor Networks (WSNs), Misdirection Attack in Wireless Sensor Network (WSN), Node Localization, Wireless Sensor Network (WSN)

1. Introduction

Wireless Sensor Network (WSN) consists of light weight remote sensors with components. These sensor nodes are generally cheaper in worth, with restricted energy storage and restricted process capabilities. Wireless Sensor Network consists of an oversized range of these sensor nodes (usually hundred or thousand of nodes). These sorts of network are to a great degree appropriated and sent in an unfriendly situations[1]. At that point gathered information is sent to the sink and sink sends information to the client through a web. Figure 1 indicated data flows from sensor node V to node S through node M and a node N to sink or destination[2].

1.1 Various Challenging Issues Involved in Wireless Sensor Network

1.1.1 Routing

The definition by routing convention is suffering from distinctive checking out reasons which can be brought about by means of the nature of WSN's. A few of these explanations are[2]:

- **Node Deployment:** Node deployment should be possible by irregular, deterministic and self-arranging. It influences the performance of Routing protocol.
- **Fault Tolerance:** WSN's are exposed to failure. The nodes should be dynamic and should not get affected on overall task[3].

1.2 Quality of Service

The QoS environment is different from conventional data network and WSN. Some of QoS challenges and issues are[3]:

- **Scalability**: The growth of the network become larger over the geographical area. So, the protocol should be scalable in terms of coverage and density of sensor nodes[3].
- **Self-Configuring**: Conditions like node failure, link failure affects the requirement of the node. Protocol design must be self-configuring and self-maintaining.

*Author for correspondence

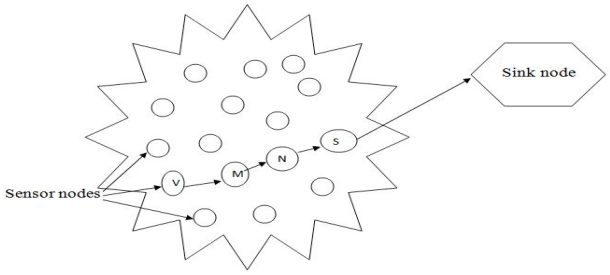

Figure 1. Wireless sensor network.

1.3 Security

Security is an imperative testing issue in WSN. The Wireless Sensor Network is helpless against security attacks as a result of the broadcast nature of the transmission medium[4]. Its primary goal is to ensure the information or data going through the sensor hub of the system or between the sensors and the base station. The basic categories of attack are eavesdropping. The former approach is called passive eavesdropping and later approach is called active approach[4].

1.4 Energy Consumption

In WSN, energy is the main constraint. The operations of sensor nodes such as data processing and transmission are energy consuming. It is easy to drain the energy during network operation. For example, in a field surveillance application, sensor nodes are distributed. Recharging or changing the node batteries is unattainable. A lot of examinations have centered on expanding the life span of the networks. The energy utilization is lessened with proficiency through right cluster head's decision and message minimization[5].

2. Attacks in Wireless Sensor Network

There can be number of malignant attacks which are confronted with remote sensor systems on Network layers which can be characterized as beneath.

2.1 Cloning Attack

It (in like manner called node replication assault) is an amazing assault in WSNs. In this assault, a foe gets only two or three nodes, copies them and after that passes on an optional number of reproductions all through the framework. The catch of nodes is possible in light of the way that sensor nodes are normally unprotected by physically ensuring due to cost considerations and are consistently left unattended after a course of action. If we don't perceive these imitations, the framework will be defenseless against an unlimited class of insider assaults. For example, the enemy now can find the action passing the reproductions (which may contain the after determining zones of officers), implant false data into the framework (which may be a false summons), attack distinctive modes and even disavow true legitimate nodes[6].

2.2 Sinkhole Attack

In this, the enemy's point is utilized to draw all the action from a particular district through a bargained hub, making an allegorical sinkhole with the adversary in the center. Sinkhole assaults routinely work by making a traded off hub look especially speaking to envelop hubs with respect to the coordinating figuring. Sinkhole assaults are difficult to counter in light of the way that coordinating information supplied by a hub is difficult to affirm. As a case, a portable workstation class adversary has a strong, powerful radio transmitter that licenses it to give a superb course by transmitting with enough vitality to accomplish a wide district of the system[7] as appeared (Figure 2).

2.3 Wormhole Attack

In this, the attacker gets packets from one point in the system, advances them through a remote or wired link with low latency in the system. Along these lines, a default link is utilized by the attacker as a part of the system. With the assistance of this link, attacker transfers a packet to another area in the system[8] as shown in Figure 3.

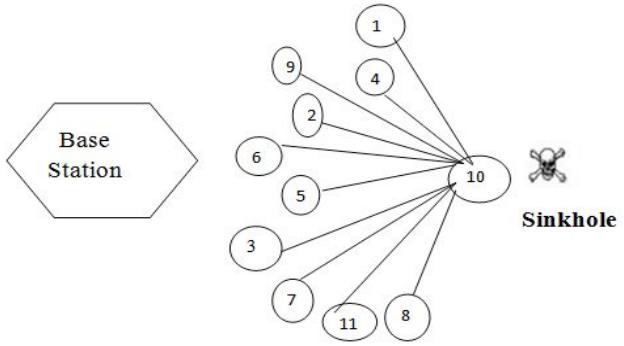

Figure 2. Sinkhole attack.

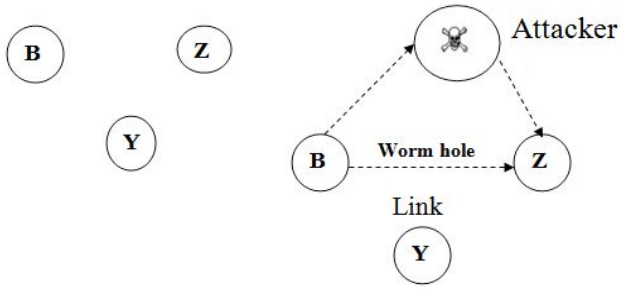

Figure 3. Wormhole attack.

2.4 Sybil Attack

This attack is a systematic risk presented by one or many malicious nodes to pronounce various unlawful recognizes to befuddle or even fall the system applications. A Sybil attack is an attack which makes different personalities from the same malicious node. In a Sybil attack, an attacker makes a few illegitimate personalities in sensor organizes either by manufacture or taking the characters of genuine nodes[9].

3. Related Work

In[10], planned innovative Message Observation Mechanism (MoM) to distinguish as well as safeguard the DoS assault. In view of the spatial-temporal correspondence, MoM uses the similarity function to distinguish the substance attack and additionally the recurrence assault. The MoM receives rekey and reroute countermeasures to confine the malevolent node. The defense investigation verifies and resistances the DoS assault as well as it is capable of diminishing the energy utilization. In[11] studied ananother approach to manage security in multi-hop code, creators present the dispersal convention. They organize privacy and DoS-fault resistance in a multi-hop code dispersal convention. The philosophy depends upon the occurrence of the Deluge, an open source, best in class code scattering convention for WSNs. Furthermore, a performance assessment is given in the plan and compared with the original Deluge and the current secure Deluge. In[12] verified how the proactive and reactive protocol scope with malevolent internal assaults (i.e., Misdirection assault) and whether one sort of protocol suggests characteristically enhanced resistance to the different assault than the feather. In[13], portrays that we can overcome numerous dangers utilizing presented encryption and verification methods and different systems can ready network administrators of ongoing assaults or activate procedures to preserve energy on influenced gadgets. In[14], suggested TARF, a Trust-Aware Routing Framework for Wireless Sensor Networks, to protect multi-hop directing in Wireless Sensor Networks beside trespassers abusing the replay of directing data with trusted organization, TARF allows a node to keep track of the trustworthiness of its neighbors and along these lines to choose a dependable course. No longer just does TARF bypass those malevolent nodes abusing different nodes personalities to mislead network traffic, it additionally achieves productive energy utilization. In[15], the target on the protection of Wireless Sensor Network with the conclusion that the defense of huge frameworks ought to be persistently reassessed to consider new recognitions. The level of security required for the application ought to likewise be checked while inclining toward hardware. In[16], addressed the harmful sort of DoS assault known as PDoS (Path-based Denial of Service) in which a foe overpowers sensor nodes extended separation away by flooding the node with replayed packets or infuses forged parcels. An answer utilizing 1-way hash chains to ensure end-to-end correspondences in Wireless Sensor Network against PDoS assaults is planned. The arrangement gave is lightweight endures burst parcels losses and container without much of a stretch be executed in advanced WSNs. In[17], energy proficient three level clustering plan presented as taking into account weighted probabilities for the decision of cluster heads. This new protocol contrasts its performance and LEACH protocol in the nearness of heterogeneity. It has three sets of nodes, super nodes, advanced node and normal node. Every node has diverse weight probabilities, taking into account these probabilities the threshold is acquired that is utilized to choose the cluster heads in each round. It exploits heterogeneity by utilizing the additional energy of super node therefore diminishes the unstable region and expansions the stable region.

4. Misdirection Attack in Wireless Sensor Network

It is the most standard DoS assault. This assault is able to be accomplished in various ways. A malignant node could disprove a significant course to a particular node in this way refuse help to the destination[18].

4.1 Sorts of Misdirection Assault

Misdirection assault can be accomplished in two ways:

- **Packets onward to a Node close toward the Destination**: This sort of misdirection assault is

fewer genuine, in light of the fact that packets compass to the destination, however from the other course which helps conveys long postpone, thus lessening throughput of the framework (bit trade each second)[18,19].

- **Packets onward to a Node far off as of the Destination**: This sort of misdirection assault is astoundingly ruinous in light of the way that all packets are sent to a node far away, thwarting them to accomplish the destination so parcels won't accomplish destination. Due to the assault, the postponement gets the opportunity to be boundless and further results in zero throughputs[18,19]. From this time forward misdirection assault is perilous in temperament as their basis defilement in execution of the network.

5. Proposed Methodology

The Wireless Sensor Network is the kind of system in which sensor nodes are passed on to sense natural conditions like temperature, weight, weight etcetera. The sensor system is the decentralized sort of system as a result of which diverse kind of security assaults is possible in the network. The security attacks are conceivable on the grounds that some malicious nodes may join the network. In this work, range based node localization technique is proposed which will identify malicious nodes, which are capable of triggering misdirection attack in the network.

5.1 Node Localization

The procedure of assessing the unknown node position inside the network is alluded to as node self-localization. Node localization is of two sorts: Range-based node localization and range-free localization. Range-free localization is algorithms rely upon proximity sensing or availability information on assessing the node areas. Range-based node localization algorithm gauges the distance between nodes as far as Time of Arrival (ToA), Time Difference of Arrival (TDoA), Received Signal Strength Indicator (RSSI) and Angle of Arrival (AoA).

5.1.1 Time-based Technique (ToA, TDoA)

These techniques are used for the calculation of the distance which is done by changing the time of propagation between two nodes with known signal propagation speed.

5.1.2 Angle of Arrival (AoA)

Angle of Arrival is also known as Direction of Arrival. These techniques are used to evaluate and measure position by geometric relationships with angles where signals are received. ToA, AoA, TDoA has better accuracy than RSSI techniques. This is due to the environmental affective factors.

5.1.3 Triangulation

The direction of a node is evaluated using this technique rather than the distance between the nodes in AoA system. Therefore, the new position of nodes is calculated using trigonometric functions.

5.1.4 Maximum Likelihood (ML) Estimation

ML estimation surveys the nodes position by diminishing the distinction between measured separations and assessed distances. Furthermore, range-based localization is likewise partitioned into two categories:

- To start with a category is to compute the distance by one hop.
- The Second category is to ascertain the distance by multi-hop. In this category, the node doesn't discuss straightforwardly with beacons. Therefore, through reference point nodes information can be gotten and moved in multi-hop correspondence. The accuracy of range based node localization is more than range free node localization.

5.2 Procedure

The following strides are followed for the recognition of malicious nodes:

- Deploy Wireless Sensor Networks with finite number of sensor nodes.
- Apply LEACH protocol for cluster entire network and in every cluster selects cluster head on the premise of distance and energy.
- Select shortest path from source to sink on the premise of reactive routing protocol.
- Apply technique of node localization to detect malicious nodes from the network.
- Isolate detected malicious nodes and re-build up the path from source to sink.

As portrayed in the flowchart (Figure 4), the network is deployed with the finite number of sensor nodes. The

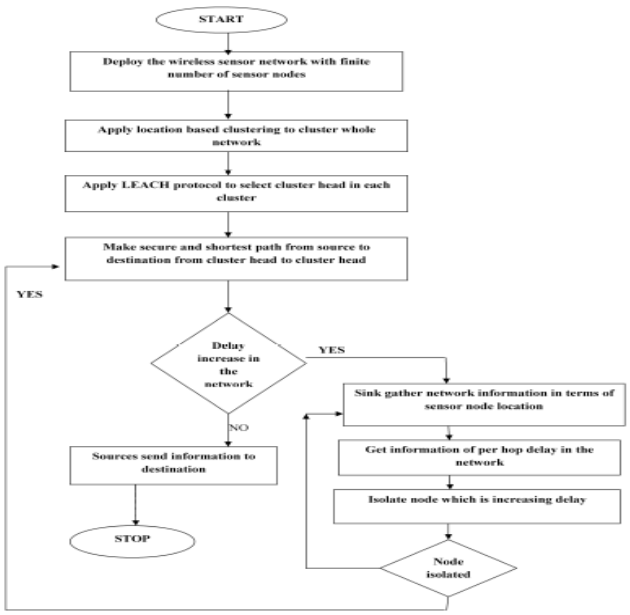

Figure 4. Flow chart of proposed methodology.

entire network is partitioned into altered size clusters. The shortest path will be built up from source to destination through the cluster heads. The node localization technique is connected which will identify the malicious node from the network. The node localization will apply in which base station will assemble node information as far as their coordinates and distance from the base station. The base station will compute delay per hop and node which is expanding delay per hop will be distinguished as the malicious node from the network.

5.3 S-LEACH Algorithm

Start ()

- Deploy the Wireless Sensor Network with an altered number of mobile nodes and in settled region.
- Divide entire network into altered size clusters send select cluster head in every cluster.
- Cluster head selection ().
  a. node=0 /// Node identification
  b. For (i=0; i<n; i++)
    a. If (distance and energy (a(i))<a(i+1);
    b. Node =a (i);
    Else
    Node=0;
    End
- The shortest path will be established bythe cluster head to sink
- Verify secure path ()

a. Get coordinates of node whose id is 0
b. For (i=0; i<n; i++)
c. a (i) = a (i-1);
d. End
e. Calculate distance between all nodes ()
a. Distance = $(a\times (i+1) - a(i))^2+(a(y+1)-a(y))^2$

- If (any nodes adjacent node! = saved information).
- That node will be detected as malicious node in the network.

End

6. Experimental Results

In this work, node localization technique is applied to detect malicious node from the network. The novel technique is implemented in NS2. The NS2 is the event-based simulator and X graphs are used to analyze network performance. As shown in Table 1, the various parameter values which are used for the simulation.

6.1 Experimental Results

The whole scenario is implemented on NS2.

As shown in Figure 5, the comparison of LEACH, Attack and proposed technique is shown in terms of delay. It is being analyzed that delay in the attack scenario is maximum and delay is reduced in the proposed scenario due to an isolation of attack in the network.The red line represents the delay in the network when misdirection attacks intriggering in the network. The green line represents the network delay in the LEACH protocol and the blue line represents the delay in the network when an attack is isolated from the network. This graph the x-axis represents time and the y-axis represents the number of packets.

Table 1. Simulation parameters

Elements	Description
Antenna type	Omi directional
MAC layer	802.11
Number of nodes	20
Link layer type	LL
Channel type	Wireless channel
Area	800*800
Routing protocol	AODV
Simulator	NS2 version 2.34

As shown in Figure 6, the correlation of the proposed, LEACH and attack scenario is appeared as far as energy. It is being broken down that energy consumption of the proposed scenario is minimum when contrasted with LEACH and attack scenario. The red line represents the energy consumption in the network when misdirection attacks in triggered in the network. The green line represents the network energy consumption in the LEACH protocol and the blue line represents the energy consumption in the network when an attack is isolated from the network. This graph the x-axis represents time and the y-axis represents energy consumption in joules.

As shown in Figure 7, the comparison of LEACH, attack and proposed scenario is shown in terms of throughput. It has been analyzed that the throughput of the proposed scenario is maximum as compared to other two scenarios. The red line represents the throughput in the network when misdirection attacks in triggered in the network. The green line represents the network throughput in the LEACH protocol and the blue line represents the throughput in the network when an attack is isolated from the network. This graph the x-axis represents time and the y-axis represents the number of packets

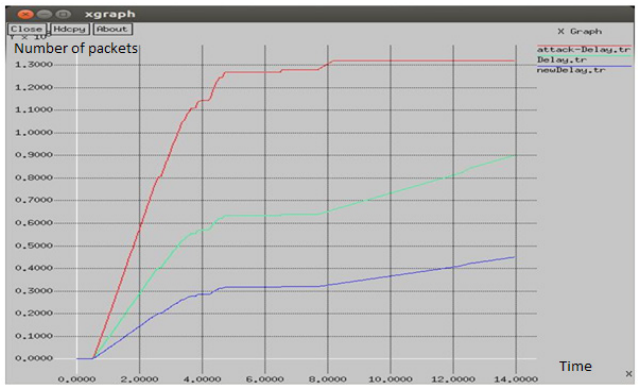

Figure 5. Comparison of LEACH, attack and proposed technique in terms of delay.

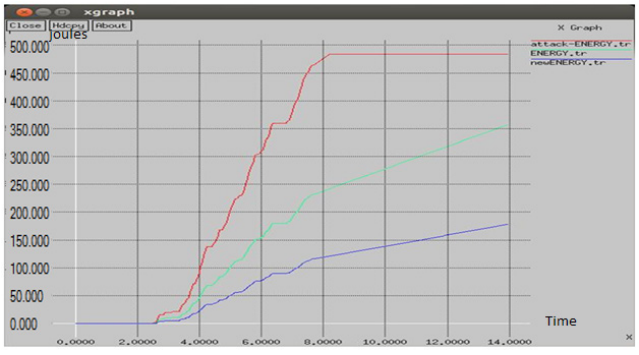

Figure 6. Comparison of LEACH, attack and proposed technique in terms of energy.

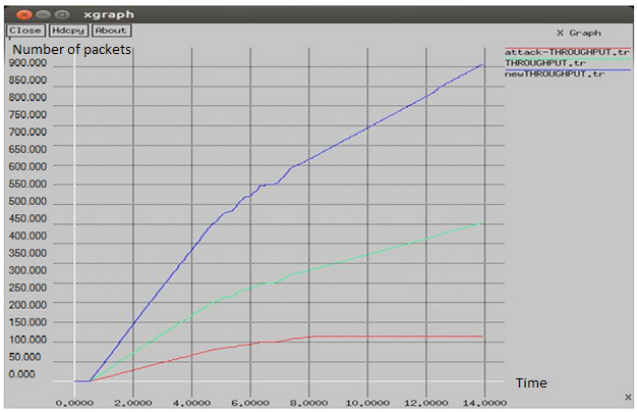

Figure 7. Comparison of LEACH, attack and proposed technique in terms of throughput

7. Conclusion

Due to self-configuring nature of sensor networks some malicious nodes may join the network which is responsible for triggering various types of active and passive attack. The misdirection attack is the active type of assault, which will increase the delay in the network. In this work, a technique has been proposed which can detect and isolate malicious nodes from the network which is responsible for triggering misdirection attack. The proposed technique is based on node localization in this method base station will analyze the delay per hop. The node which can increase delay maximum times will be detected as malevolent nodes in the network. It is analyzed that the energy consumption of the network gets reduced, throughput gets increased and delay gets reduced in the network. Towards the end performance parameters are assessed on the premise of delay, throughput, and energy.

8. References

1. Supriya D, Ripul R. Review on LEACH-homogeneous and heterogeneous wireless sensor networks. International Journal of Innovative Research in Computer and Communication Engineering. 2015; 3(5):4442–7.
2. Ganesh S, Amutha R. Efficient and secure routing protocol for wireless sensor networks through SNR based dynamic clustering mechanisms. IEEE Journal of Communications. 2013; 15(4):422–9.

3. Vanita R, Renu D. A study of ad-hoc network: A review. International Journal of Advanced Research in Computer Science and Software Engineering. 2013; 3(3):135–8.
4. Reji M, Kishore Raja PC, Joseph C, Baskar R. Performance metrics of wormhole detection using path tracing algorithm. Indian Journal of Science and Technology. 2015 Aug; 8(17):1–9.
5. Durairaj M, Persia A. ThreV - An efficacious algorithm to thwart MAC Spoof DoS attack in wireless local area infrastructure network. Indian Journal of Science and Technology. 2014 Jan; 7(5):581–8.
6. Robert AE, Hemalatha M. Epidemic dynamics of malicious code detection architecture in critical environment. Indian Journal of Science and Technology. 2014 Jan; 7(6):770–5.
7. Uddin M, Alsaqour R, Abdelhaq M. Intrusion detection system to detect DDoS attack in gnutella hybrid P2P network. Indian Journal of Science and Technology. 2013 Feb; 6(2):4045–57.
8. Pathan ASK, Lee HW, Hong CS. Security in wireless sensor networks: Issues and challenges. IEEE 8th International Conference Advanced Communication Technology, ICACT'06; Phoenix Park. 2006. p. 1043–8.
9. Padmavathi DG, Shanmugapriya D. A survey of attacks security mechanisms and challenges in wireless sensor networks. International Journal of Computer Science and Information Security. 2009; 4(1):1–9.
10. Zhang YY, Li XZ, Liu Y. The detection and defense of DoS attack for wireless sensor network. The Journal of China Universities of Posts and Telecommunications. 2012; 19(2):52–6.
11. Hailun T, Diethelm O, Zic J, Sanjay J. A confidential and DoS-resistant multi-hop code dissemination protocol for wireless sensor network. Proceedings of the 2nd ACM Conference on Wireless network Security; 2009. p. 245–52.
12. Yau PW, Hu S, Mitchell CJ. Malicious attacks on ad hoc network routing protocols. International Journal of Computer Research. 2007; 1–24.
13. Raymond DR, Midkiff SF. Denial-of-service in wireless sensor networks: Attacks and defenses. IEEE Pervasive Computing. 2008; 7(1):74–81.
14. Zhan G, Shil W, Deng J. TARF: A trust-aware routing framework for wireless sensor networks. Proceeding 7th European Conference ESWN'10; Portugal. 2010. p. 65–80.
15. Modares H, Rosli S, Moravejosharieh A. Overview of security issues in wireless sensor networks. IEEE 2011 3rd International Conference on Computational Intelligence, Modelling and Simulation; Langkawi. 2011. p. 308–11.
16. Deng J, Han R, and Mishra S. Defending against path based DoS attacks in wireless sensor networks. ACM Proceedings of the 3rd ACM Workshop on Security of ad hoc SASN'05; 2005. p. 89–96.
17. Lindsey S, Raghavendra CS. PEGASIS: Power efficient gathering in sensor information systems. IEEE Aerospace Conference Proceedings; 2002; 3:1125–30.
18. Sachan RS, Wazid M, Avita K, Singh DP, Goudar RH. A cluster-based intrusion detection and prevention technique for misdirection attack inside WSN. IEEE International Conference on Communications and Signal Processing (ICCSP); Melmaruvathur. 2013. p. 795–801.
18. Heinzelman W, Chandrakasan A, Balakrishnan H. Energy-efficient communication protocol wireless microsensor network. Proceedings of 33rd Hawaii International Conference on System Sciences; 2000. p. 1–10.