A DISTRIBUTED NOVEL HYBRID INTRUSION DETECTION FRAME-WORK

Elango P.E.
Ph.D Research Scholar, PG & Research Dept Of Computer Science,
Periyar University, Salem, India.
Subbaiah S
Assistant Professor, Department Of Computer Applications,
Vivekananda College Of Arts & Science (Autonomous), India

Abstract

To protect from these attacks various intrusion detection techniques have been developed. The prosperity of technology worldwide has made the concerns of security tend to increase rapidly. The enormous usage of internetworking has raised the need of protecting system(s) as well as network(s) from the unauthorized access (intrusion). To tackle the intrusive activities, several countermeasures have been found in literature viz. firewall, antivirus and currently widely preferred Intrusion detection System (IDS). IDS, is a detection mechanism for detecting the intrusive activities hidden among the normal activities. The revolutionary establishment of IDS has attracted analysts to work dedicatedly enabling the system to deal with technological advancements. In this paper proposed into LIDeA IDS agent architecture and Local Detection Engine Module may be expected as another step towards advancement of IDS. The framework utilizes the crucial data mining classification algorithms beneficial for intrusion detection.

Keywords: Intrusion, Key Management, Detection Module, Wireless Sensor Network.

1. Introduction

A vision is emerging of the convergence of wireless communications, embeddedsensing and processing devices with distributed algorithms into the field of wireless sensor networks (WSNs). The proponents of this emerging technology envisiona future in which environments from nature reserves to cities are instrumentedwith disposable computing nodes, each with an onboard radio transceiver, battery, environmental sensors and processing capabilities. Wireless sensor network research grew out of the distributed sensor networks project at the Defence Advanced Projects Research Agency (DARPA), although thetechnology of the 1970s limited processing and communications and restricted thenodes to large form factors. With the exponential progress and cost reductionin micro-processing during the 1990s and 2000s, many new applications for WSNdeployment emerged. The Amorphous Computing project envisioned highlygeneric, cheap and indistinguishable miniature devices, operating by analogy to theindividual cells of biological systems. Since then, deployment of wireless sensor networks has been considered for diversespectrum domains, including logistics, medicine, environmental monitoring, military monitoring and surveillance. Surveys of WSN concepts andtechnology illustrate the directions taken in the literature. Each node in a wireless sensor network is a self-contained unit comprised of a power supply (generally batteries), a communication device (radio transceivers), a sensor or sensors, analog-to-digital converters (ADCs), a microprocessor, and data storage. The nodes self-organize themselves, into wireless sensor networks and data from the nodes is relayed to neighboring nodes until it reaches the desired destination for further processing. Recently, the WSN's technology has widely been used in our daily life. A typical WSN is shown in Figure 1. In Figure 1 an event is detected in the sensor field and the information is routed to the sinker or base station then to the user with several communication media.

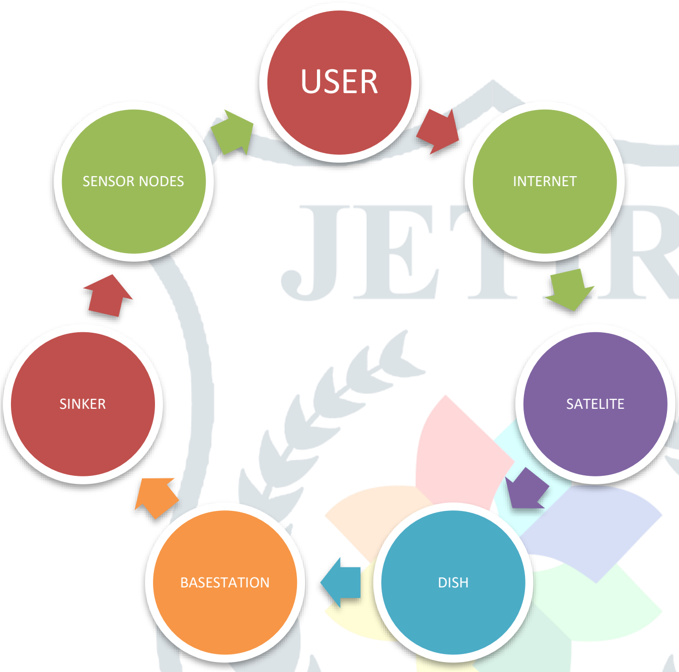

Figure 1: Traditional Wireless Sensor Network flow

Wireless Sensor Networks have been applied to a range of applications, monitoring of space which includes environmental and habitat monitoring, indoor climate control, surveillance. Monitoring things example can be outlinedas structural monitoring, condition-based equipment maintenance. In addition, monitoring the interactions of things with each other and the surrounding space e.g., emergency response, disaster management, healthcare, energy sector. The majority of these applications may be split into two classifications: data collection and event detection.

2. Literature survey

AUTHOR NAME	METHOD	ADVANTAGES
Asmaa Shaker Ashoor, Prof. Sharad Gore	Then the detection appeared and audit data and its importance led to terrific improvements in the subsystems of every operating system.	IDS and Host Based Intrusion Detection System (HIDS) were first defined. SRI International and Dorothy Denning began working on a government project

		that launched a new effort into intrusion detection system development
Inayat, Z., Gani, A., Anuar, N.B.Anwar, S., Khan, M.K	Attacks can be said to be adversarial intrusions against IDS or simply a set of actions that violate the security policies associated with the IDS itself	Despite the development of several defensive techniques such as cryptography, firewalls, and access control for secure communication, these anti-threat systems currently possess limitation in detecting intrusion attacks. Therefore, an IDS with appropriate countermeasures, such as an intrusion response system (IRS), is essential for detecting and responding to potential intrusions and attacks
Scarfone, K.Mell	IDSs are the hardware or software systems that autonomously identify and response in-appropriate events (such as intrusion attacks) occur in computer systems.	Depending on IDS settings and configurations, IRSs can continuously monitor system health and apply suitable countermeasures to identify and respond to potential incidents and inappropriate activities effectively and hence ensures optimal security in any computing environment
Wu, Z., Xu, Z., Wang, H	The application layer includes Algorithms of 24 host-based attacks such as spamming, race condition attacks, buffer overflow attacks, mail forgery, and man-in-the-middle attacks. Host-based attacks are mostly attacks against system availability, operating systems performance, and web service operations	Network-based incidents include attacks on networks aimed at affecting network availability and performance. Unlike in wired networks, in which attackers target victim networks through firewalls and gateways, attackers of wireless ad hoc networks usually gain access from several access point and target any open node
Ragsdale, D.J.; Carver, C.A.; Humphries, J.W.; Pooch, U.W	An IDS basically generates an alert in the form of a report and notification upon the detection of an intrusion. Without an appropriate security countermeasure, IDS is useless. A response system should be integrated with IDS to assist and find the source of an attack.	An IDS is classified as either passive or active depending on the response system. Passive response is further divided into notification and manual response, whereas active response is considered automatic. Similarly, an IRS has three main types: notification, manual, and automatic

Raju, P.N	The Simple Network Management Protocol traps and reports generate alarms to network management systems. Using a proper IRS in the form of an antivirus that supports the entire network infrastructure can help with responding to intrusions within a specific timeframe.	IRS the response is always dynamic based on the response parameter and attack nature. During the selection of dynamic response options, the response manager is mostly concerned about the cost of the response. The requirement of the distributed environment is mainly to have a cost-sensitive and adaptive IRS. In cost-sensitive IRS, the main contribution is that the cost of any response should always be lower than the damage cost
Hawrylkiw, D. SANS.	ICMP response is to ensure that the attacking host identifies the victim network or prevents a “requested service is unavailable” response	However, differentiating true attackers from normal users is difficult, so enabling remote logging in to another system is the best method to collect additional information about attackers. Blocking the IP addresses of specific attackers is also an alternative
Ragsdale, D.J.; Carver, C.A.; Humphries, J.W.; Pooch	An IDS is classified as either passive or active depending on the response system. Passive response is further divided into notification and manual response, whereas active response is considered automatic. Similarly, an IRS has three main types: notification, manual, and automatic	In a notification system, a response in the form of an alert and a report is generated and sent through e-mail or notification. By contrast, in a manual response system a predefined set of response options exists and is triggered by a security controller with the detection of an intrusion. In these two systems, the time duration within the detection and response activation opens an opportunity for attackers
ImenBrahmi, Sadok Ben Yahia, and Pascal	Association and correlation mining can be applied to find relationships between system attributes describing the network data.	Such information can provide insight regarding the selection of useful attributes for intrusion detection. New attributes derived from aggregated data may also be helpful, such as summary counts of traffic matching a particular pattern
Li Bo, Jiang Dong-Dong	The anomaly detection system is effective against novel or	Intrusion detection systems are also categorized according to the

	unknown attacks. There is no need of prior knowledge about specific intrusions in anomaly detection technique. One of the drawbacks of anomaly detection is the high percentage of false positives	kind of input information they analyze. So this is classified into host-based, network-based, wireless and Network Behavior Analysis (NBA) intrusion detection system.
FoongHengWai ,Yin Nwe Aye, Ng Hian James	Network Behavior Analysis which examines network traffic to identify threats that generate unusual traffic flows, such as distributed denial of service (DDoS) attacks	Certain forms of malware such as worms, backdoors, and policy violations e.g., a client system providing network services to other systems. Network behavior analysis systems are also deployed to monitor flows on an organization's internal Networks, and are also sometimes deployed where they can monitor flows between an organization's Networks and external networks such as the Internet.
LongeOlumideBabatope., Lawal, Babatunde. IbitolaAyobami,	Intrusion detection is the process of identifying and responding to malicious activities targeted at computing and network resources	An intrusion attempt, also named as attack refers to a sequence of actions by means of which an intruder attempts to gain control of a system [6]. The aim of an Intrusion Detection System (IDS) is therefore to discriminate intrusion attempts and intrusion preparation from normal system usage.
Das, K	The detector is monitoring the transition from one state to another and if the anticipated transition is different from the transition that has occurred then it is defined as anomaly.	In this section various anomaly detection methodologies for Anomaly detection has been discussed under different categories. Each of these techniques has its own advantages and disadvantages and the selection of the methods has been done based on the need. Most of these techniques assume that anomalies are rare compared to normal data. The following part of the thesis do assume the same way and in any network if the anomaly is more than 10% then it calls for a serious concern
SampadaChavan, Khusbu Shah, Neha Dave and Sanghamitra	It is an innovative approach to build a computationally	It is an information processing model that is inspired by the way

Mukherjee	intelligent system, analogous to the reasoning of human mind and ability to learn from environment under imprecision and uncertainty.	The information is processed in biological nervous systems such as brain. ANN consists of lots of processing elements called neurons working in unison to solve problems. ANN is also called as Neural Networks (NN)
Zwicky, F	Morphological analysis is simply an ordered way of looking at things	Morphological Analysis is a simple, powerful conceptual methodology widely used in linguistics, biology and technology forecasting. Today, morphology is associated with a number of scientific disciplines in which formal structure is a central issue.

3. Methodology

The agents that are hosted by the nodes are capable of sharing their partial views, agree on the identity of the source and expose it. By distributing the agents throughout the network and have they collaborate, we make the system scalable and adaptive. When a malicious node is found, an alarm message is broadcasted to the network. Each node then makes a final decision based on the detection reports from other nodes. To avoid drastic flooding over the network caused by broadcasting local detection results, the alarm messages are restricted to a region formed only by the alerted nodes.

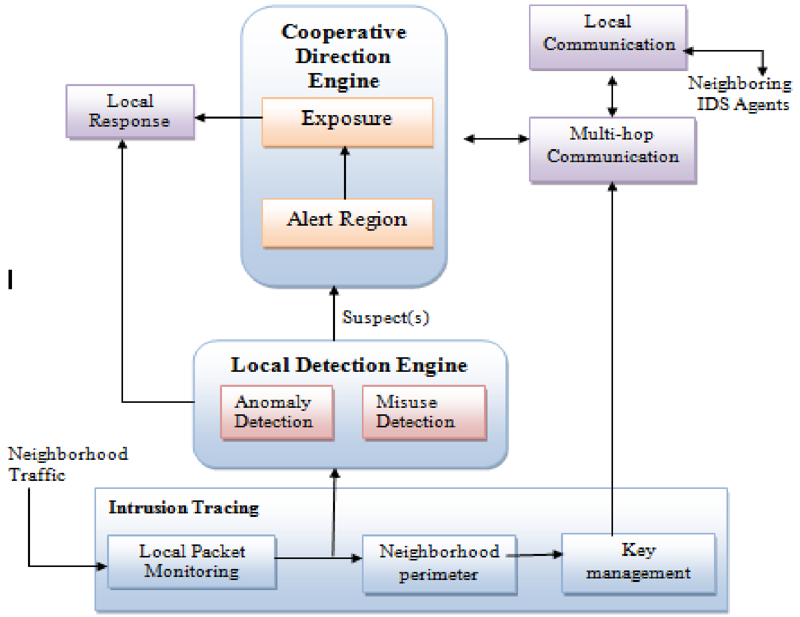

Figure 2: Architecture of LIDeA IDS agent

We build the architecture of the IDS agent based on the conceptual modules shown in Figure 2. Each module is responsible for a specific function, which we describe in the sections below. The IDS agents are identical in each node and they can broadcast messages for agents residing in neighboring nodes.

4. Neighborhood Perimeter & Key Management Module

After the deployment of the sensor network, an initialization phase takes place. During this phase all nodes discover their 2-hop neighborhood by broadcasting their IDs with a packet that has a TTL field equal to 2, meaning that each packet will be forwarded only once by the sender's 1-hop neighbors (NeighborhoodPerimetermodule). This is done because, as we described earlier, the detection process involves the communication of the nodes which are neighbors of the (yet unknown) attacker, but they might be 2-hops away from each other. The intuition behind the usage of such a key-chain scheme is to authenticate each one of thesubsequent message transmissions that hold a node's vote. Since we don't care about secrecy, as the attacker can participate in the detection process, we wish to ensure message integrity and freshness. Therefore, it is more efficient to use key chains, instead of other cryptographic primitives (e.g.,public key cryptography), as they are Novel hybrid enough to run in limited computing environmentslike the ones we encounter in sensor networks. This is based on the fact that once a sensor nodehas an authenticated key in a key chain, only pseudo random function operations are needed toauthenticate the subsequent broadcast messages.

Furthermore, key chains ensure non-forge ability and protection against old-keys compromise. Their operation is based on using different key commitments, at each run of the detection process task, and disclosing the used key (for message authentication) at the end of each round. Therefore, even in the case that one of these keys is exposed by the adversary, it doesn't give her access to any subsequent keys. As a result she may succeed in forging broadcast messages for only one detection process round. However, to improve the survivability of our scheme against such forged message attacks, we use redundant message transmission and random delays to deal with the messages that hold node votes. In this way when a node receives an incoming signed vote, it accepts it only while it has not published its own key and it has not received the key from the node that sends the message. The strength and usability of these key chains depend on the authentication of the key chain commitment contained in the corresponding commitment distribution message. At the time of key disclosure, each one of the receivers can easily verify the correctness of the key by checking whether it generates the previous one, stored in the key chain, through the application of*F*. This makes the commitment distribution messages attractive targets for attackers. An attacker may disrupt the distribution of the disclosed key messages, and thus prevent the sensors from authenticating broadcast messages during the corresponding detection process time intervals. The simplest way to do this is to jam the communication channel. However, it is not to the benefit of the attacker to jam or interfere overheard communications, since this can be detected by the base station and lead to her exposure.

4.1 Local Detection Engine Module

This module collects the audit data from the Local Packet Monitoring module and analyzes it according to some given rules. A set of rules is provided for each attack, and whenever one or more rules are satisfied, a local alert is produced by the module. Whether a rule is satisfied or not does not just depend on information from the intercepted packets, but also on information from the 2-hop neighborhood table or information from past observed behavior. Following the discussion of misuse detection catches intrusions in terms of the characteristics of known attacks or system vulnerabilities (any action that confronts to the pattern of a known attack is considered intrusive) whereas anomaly detection is based on the normal behavior of the system (any action that significantly deviates from this behavior is considered intrusive). Example of misuse detection rules includes the case of a selective forwarding attack where the nodes are able to identify the one node that drops the messages by monitoring the transmissions in their neighborhood.

In the case of anomaly detection, statistical modeling is among the earliest methods used for detecting intrusions in electronic information systems. It is assumed that an intruder's behavior is noticeably different from that of a normal user, and statistical models are used to aggregate the user's behavior and distinguish an attacker from a normal user. We explore the development of such a localized anomaly algorithm that can detect wormhole attacks on wireless networks directly based on connectivity information implied by the underlying communication graph. The intuition is to search for simple network structures that indicate that no attack is taking place. The detection engine of a node s outputs an alert. This alert can contain one of two things: either the node ID of the attacker or a list of suspected nodes. In the first case, the node detecting the attack was able to identify the source (e.g. a node dropping packets), so it directs the alert to the Local Response module for immediate measures. In the second case, it simply outputs some set Suspect(s) of possible attacking nodes. Suspect(s) will contain a subset of neighbors or may even be equal to the whole neighborhood of s. In any case, it cannot contain any non-neighboring node, since node s could not have observed an attack outside its radio range. By communicating its list of suspected nodes to the other nodes and collaborating with them is what can lead to recognizing the attacker's identity.

4.2 Local Response Module

Once the network is aware that an intrusion has taken place and has detected the compromised area, appropriate actions are taken by the *Local Response* module. The first action is to cut off the intruder as much as possible and isolate the compromised nodes. After that, proper operation of the network must be restored. This may include changes in the routing paths, updates of the cryptographic material (keys, etc.) or restoring part of the system using redundant information distributed in other parts of the network. IDS systems in other types of networks always report an intrusion alert to a human, who takes the final action. Correctly, this approach is usually neglected in WSN IDS literature. Sensor net-works should (and they actually are) able to demonstrate an autonomic behavior, taking advantage of their inherent redundancy and distributed nature. Autonomic behavior means that any response to an intrusion attempt is performed without human intervention and within finite time.

Conclusion

This research discusses the problem of intrusion detection in sensor networks that utilizes a large number of autonomous, but *localized*, cooperating agents in order to detect an attacker. The nodes use coordinated surveillance by incorporating inter-agent communication and distributed computing in decision making to collaboratively infer the identity of the attacker from a set of suspicious nodes.Despite the necessity of intrusion detection schemes for wireless sensor networks, a good solution has not yet been devised. Of course, as we mentioned, this is due largely to the resource constraints present in this type of networking. However, the demonstrated implementation details of our IDS system show that is Novel hybrid enough to run on sensor nodes, in terms of communication, energy, and memory requirements. This shows that studying the problem of intrusion detection in sensor networks is a viable research direction and with further investigation it can provide even more attractive solutions for securing such types of networks.

REFERENCES

[1] Anderson, J.P., Computer Security Threat Monitoring and Surveillance, Technical report, James P. Anderson Co., Fort Washington, PA., April 1980. On Software Engineering, vol. SE-13, pp. 222-232, February 1987.

[2] Ashok Kumar, D., and Venugopalan, S.R., 2016, December. A Novel algorithm for Network Anomaly Detection using Adaptive Machine Learning.In Advanced Computing and Intelligent Technologies (ICACIE), 2016 First International Conference on. Springer

[3] Singh, S.P. (2010) Data Clustering Using K-Mean Algorithm For Network Intrusion Detection, Thesis, Lovely Professional University, Jalandhar.

[4] Deepthy K. Denatious, and John, A. (2012) 'Survey on data mining techniques to enhance intrusion detection', International Conference on Computer Communication and Informatics, ICCI-2012, Coimbatore, India.

[5] C. Kruegel, F. Valeur, and G. Vigna. Intrusion Detection and Correlation: Challenges and Solutions. Springer-VerlagTelos, 2004.

[6] L. R. Halme and R. K. Bauer. AINT misbehaving – A taxonomy of anti-intrusion techniques. In Proc. of 18th NIST-NCSC National Information Systems Security Conference, pages 163– 172, 1995.

[7] D.E. Denning, An Intrusion-Detection Model, IEEE Transactions on Software Engineering, vol. SE-13, pp. 222-232, 1987.

[8] Dinakara K, “Anomaly Based Network Intrusion Detection System”, Thesis Report, Dept. of Computer Science and Engineering, IIT Khargpur 2008

[9] Guy Bruneau – GSEC Version 1.2f,” The History and Evolution of Intrusion Detection”, SANS Institute 2001.

[10] Ilgun, Koral, USTAT:a real time IDS for Unix, Proceedings of the 1993 IEEE Computer Society Symposium on research insecurity and privacy, 1993.

[11] Mark Crosbie, Gene Spafford, Defending a Computer System using Autonomous Agents, Technical report No. 95-022, COAST Laboratory, Department of Computer Sciences, Purdue University, March 1994.

[12] D. Anderson, T. Frivold, A. Valdes, Next-generation intrusion detection expert system (NIDES), Technical report, SRI-CSL95-07, SRI International, Computer Science Lab, May 1995."

[13] Paxson, Vern, Bro: A system for detecting network intruders in real-time, Computer Network, v 31, n 23, Dec 1999.

[14] Ning,Wang X.S, Jajodia S, Modelling requests among cooperating IDSs, Computer Communications, v 23, n 17, Nov, 2000."

[15] J. E. Dickerson and J. A. Dickerson, “Fuzzy network profiling for intrusion detection,” In Proceedings of the 19th International Conference of the North American Fuzzy Information Processing Society (NAFIPS), 13-15 July 2000, pp. 301 – 306.

[16] TEODOR-GRIGORE LUPU,” Main Types of Attacks in Wireless Sensor Networks “

[17] Sunil Gupta,Authentication Framework against “Malicious Attack in Mobile Wireless Sensor Networks”, Vol II, IMECS 2017, March 15 - 17, 2017

[18] Chaudhari H.C. and KadamL.U,”Wireless Sensor Networks: Security, Attacks and Challenges International Journal of Networking” ,Volume 1, Issue 1, 2011, pp-04-16

[19] Hu, Perrig, and Johnson, “Malicious Node Detection in Wireless Sensor Networks” WaldirRibeiroPiresJ´uniorThiago H. de Paula FigueiredoHao Chi Wong Antonio A.F. Loureiro

[20] DeepmalaVerma, Gajendra Singh, KailashPatidar, Detection of Vampire Attack in Wireless Sensor Networks , Vol. 6 (4) , 2015, 3313-3317

[21] L. Lamport.” Constructing digital signatures from one-way function”.in technical report SRI-CSL-98, SRI International, Oct. 1979.

[22] Dr. AdwanYasin ,KefayaSabaneh ,"Enhancing Wireless Sensor Network Security using Artificial Neural Network based Trust Model" , Vol. 7, No. 9, 2016

[23] H. Gorine, M. Ramadan Elmezughi, "Security Threats on Wireless Sensor Network Protocols," 18-19 August 2016

[24] SoramRakeshSingh ,NarendraBabu C R,Improving the "Performance of Energy Attack Detection in Wireless Sensor Networks by Secure forward mechanism", Volume 4, Issue 7, July 2014

[25] D. I. Curiac, O. Banias, F. Dragan, C. Volosencu and O. Dranga, "Malicious Node Detection in Wireless Sensor Networks Using an Autoregression Technique," 3rd International Conference on Networking and Services, Athens, 19-25 June 2007, p. 83

[26] DelPHI: "worm hole detection mechanism for ad hoc wireless network proposed" by Hon Sun Chiu and King-Shan Lui in international Symposium on wireless Pervasive Computing ,Phuket, Thailand, 16-18 january 2006.

[27] H.Chen, H.Wu, X.Zhou,"Reputation-based Trust in Wireless Sensor Network", in IEEE International Conference on Multimedia and Ubiquitous Engineering, 26th -27th April, (MUE'07), 2007, Shanghai.,pp.603-607.

[28] AndriyStetsko, Lukas Folkman, VashekMatyas, Neighbor-based" Intrusion Detection for Wireless Sensor Networks", 6th International Conference on Wireless and Mobile Communications (ICWMC), 2010, pp. 420-425

[29] Abdul Wahid PavanKumar,"A Survey On Attacks, Challenges and Security Mechanisms In Wireless Sensor Network" .

[30] International Telecommunications Union (ITU-T), Recommendation X.200 (07/94): Open Systems Interconnection - Basic Reference Model, July 1994.

[31] I. Demirkol, C. Ersoy, and F. Alagoz, MAC protocols for wireless sensor networks: a survey IEEE Communications Magazine, vol. 44, pp. 115{121, Apr. 2006.

[32] J. Hill, R. Szewczyk, A. Woo, S. Hollar, D. Culler, and K. Pister, System architecture directions for networked sensors ACM SIGPLAN Notices, vol. 35, pp. 93{104, Nov. 2000.

[33] P. Gupta and P. R. Kumar, The capacity of wireless networks IEEE Transactions on Information Theory, vol. 46, pp. 388{404, Mar. 2000.

[34] T. Melodia, M. Vuran, and D. Pompili, The State of the Art in Cross- Layer Design for Wireless Sensor Networks in Wireless Systems and Network Architectures in Next Generation Internet (M. Cesana and L. Fratta, eds.), vol. 3883 of Lecture Notes in Computer Science, pp. 78{92, Springer Berlin, 2006.

[35] P. Skraba, H. Aghajan, and A. Bahai, Cross-Layer Optimization for High Density Sensor Networks: Distributed Passive Routing Decisions in Ad-Hoc, Mobile, and Wireless Networks (I. Nikolaidis, M. Barbeau, and E. Kranakis, eds.), vol. 3158 of Lecture Notes in Computer Science, pp. 630{644, Springer Berlin, 2004.

[36] S. Biswas and R. Morris, ExOR: opportunistic multi-hop routing for wireless networks SIGCOMM Computer Communications Review, vol. 35, pp. 133{144, Aug. 2005.