Mobile Agent Based Hierarchical Intrusion Detection System in Wireless Sensor Networks

Surraya Khanum[1], Muhammad Usman[2] and Ala'a Alwabel [3]

[1] Department of Computer Science & Information Systems, Faculty of Computer Science
King Khalid University, Abha, Kingdom of Saudi Arabia

[2] Department of Computer Science, Faculty of Computer Science
King Khalid University, Abha, Kingdom of Saudi Arabia

[3] Department of Information Systems, Faculty of Computer Science
King Khalid University, Abha, Kingdom of Saudi Arabia

Abstract

Security mechanism is a fundamental requirement of wireless networks in general and Wireless Sensor Networks (WSN) in particular. Therefore, it is necessary that this security concern must be articulate right from the beginning of the network design and deployment. WSN needs strong security mechanism as it is usually deployed in a critical, hostile and sensitive environment where human labour is usually not involved. However, due to inbuilt resource and computing restriction, security in WSN needs a special consideration. Traditional security techniques such as encryption, VPN, authentication and firewalls cannot be directly applied to WSN as it provides defence only against external threats. The existing literature shows that there seems an inverse relationship between strong security mechanism and efficient network resource utilization. In this research article, we have proposed a Mobile Agent Based Hierarchical Intrusion Detection System (MABHIDS) for WSN. The Proposed scheme performs two levels of intrusion detection by utilizing minimum possible network resources. Our proposed idea enhance network lifetime by reducing the work load on Cluster Head (CH) and it also provide enhanced level of security in WSN.

Keywords: *Wireless Sensor Networks, Mobile Agent, Network Security, Intrusion Detection System, Hierarchical IDS.*

1. Introduction

Wireless Sensor Network (WSN) is an emerging technology [1,2]. The WSN is generally deployed in a critical and hostile environment where the human labour is not implicated. Some of the trendy applications of WSN are fire response, traffic monitoring, military command etc. [1,2,3,4].

Different types of network topologies such as star, tree, mesh etc are used for communication in WSN. In a cluster based hierarchical approach, concentration of sensor nodes forms a cluster and one node among them acts as a Cluster Head (CH). The CH assumes to have a larger battery and acts as a supervisor node for communication between other nodes. All CH in the network are connected to a Base Station (BS) which is a single decision making authority. One of the cluster topology is depicted in figure 1.

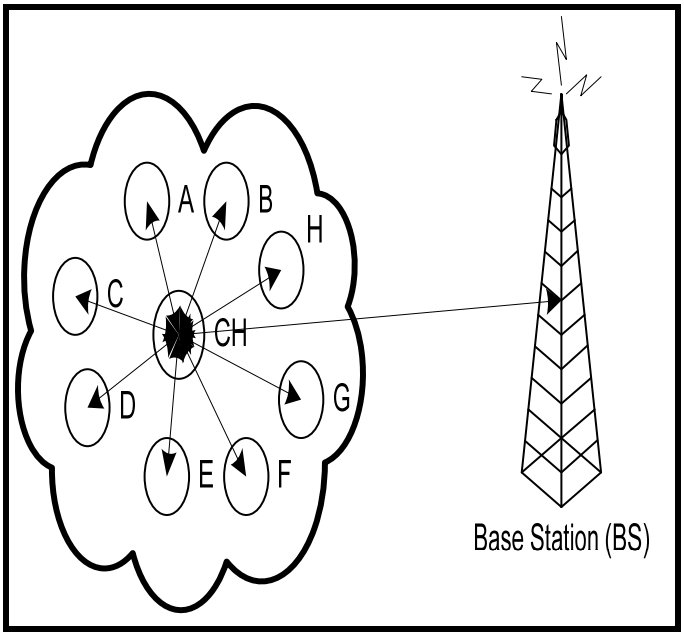

Fig. 1 Cluster in a sensor network.

The CH is a special sensor node with the specific tasks of receiving, processing, storing and forwarding data collected from the member nodes of that specific cluster. Each CH must be connected with Regional Head (RH) or BS, depending on the deployment scheme of the WSN. The RH

works very much like CH, but unlike CH, the RH connects different CH together. All the RH in the network is connected to BS which is a central governing and decision making authority. In a typical deployment of wireless sensor network, there are three tiers. At the top tier BS is deployed, RH and CH comes at middle tier, whereas the sensor node comes at lower most tiers.

Security is a major challenge in WSN networks. Deployment of adequate security mechanism in WSN is critical due to its resource restricted nature. Traditional security techniques such as encryption, VPN, authentication and firewalls are inadequate for WSN as they provide protection only against external threats and resource hungry in nature. Consequently more sophisticated techniques are required to monitor and discover intrusions in WSN as these networks are usually deployed in critical and real time application.

To protect the network against the intrusion customarily there are two types of defensive approaches. These are known as static and dynamic defensive approaches [3]. Firewalls, VPN, authentication and encryption are common examples of static technique. They only provide security from external threats and called as first line of defence. If a node inside the network is compromised, the whole security will be compromised. Therefore there is a need of better security mechanism that prevents the network from both internal & external threats.

An Intrusion Detection System (IDS) is a dynamic monitoring system used to identify, examine and observe violated activities. It discovers breach and illegal access to confidentiality, unavailability, authorization, authentication, integrity and network resources [4].

The related works shows that there exist a trade-off between better security mechanism and efficient resource utilization of sensor networks. If we increase network security we have to compromise on efficient resource consumption and vice versa. As a result, better security mechanisms is required that uses network resources efficiently. In order to tackle with this issue, we have proposed a Mobile Agent Based Hierarchical Intrusion Detection System (MABHIDS). Our proposed scheme uses minimum network resources by providing enhanced level of security.

The rest of the paper is organized as; in section II we have discussed the related work. Section III is about proposed scheme. We have discussed advantages of the proposed scheme in section IV. In section V, we have evaluated the performance of proposed scheme. In section VI we have concluded the contribution of this research paper. Finally, the list of references is given in section VII.

2. Related Work

We have divided the survey of existing literature into five categories. These categories are Domain Introduction, Architecture of WSN, Security issues on WSN, Different security mechanisms in WSN and Applying IDS to WSN.

In domain introduction we have surveyed different research papers regarding WSN introduction. The WSN is an autonomous network to monitor physical and environmental situation. A gateway incorporates WSN to the other wired/wireless networks. They are usually deployed for monitoring critical application such as structural monitoring for buildings and bridges, industrial machine monitoring, process monitoring, asset tracking etc.

Three types of network topologies are used in WSN: Star, Cluster tree and Mesh network. In star topology each sensor is directly connected to gateway. In cluster tree the sensor nodes form a tree structure and the higher node is connected to the gateway. The data flows from lower level of node to the higher level of node [3, 5]. In mesh network each sensor node is directly connected to other sensor node forming a net of interconnection link with each other.

The existing literature regarding WSN architecture shows that the sensor nodes have lack of common framework with no standardization in protocol for communication. There exist no interoperability mechanisms between two components of sensor nodes developed by different companies [5]. The sensor node is composed of battery so resource aware protocol architecture is needed for efficient communication. They use by default broadcast medium for communication which increases the risk of network congestion. Similarly, the authors have outlined the physical architecture, power management, commercially available sensor nodes and their characteristics in [6].

We have performed an in-depth survey regarding security issues in wireless sensor networks[7,8,9,10,11,12,13,14,15]. The authors argue that security is a major concern in any type of network particular in WSN. The WSN have resource restriction constraint i.e. limited energy, low computation capability, small memory, vulnerable to physical capture and insecure nature of wireless communication channel. All this limitation makes security in WSN a challenging issue.

The authors have outlined the basic security requirement, threat model and security attacks. They have divided the security issues into five categories: cryptography, key management protocols, security, routing, secure data aggregation and intrusion detection along with their advantages and shortcomings. The authors have discussed security requirement i.e. data authentication, data

confidentiality, data integrity, data freshness, self organization, availability, time synchronization, secure localization, scalability, availability, accessibility and flexibility. They have examined different types of security attacks i.e. Sybil, Denial of Service (DoS), physical, node replication, privacy violation and traffic analysis. The authors have provided basic guidelines and defensive measures against these types of attacks. They observed the DoS threats and layer wise security problems and argued that limited resources make encryption keys and digital signatures inadequate for securing WSN. Further, notify that there is a trade-off between energy and communication distance between sensor nodes therefore it should also be well managed.

Then we surveyed different existing security mechanisms in WSN. In [16] the authors assumed that base station is capable for storing all cryptography keys having sufficient memory and battery power. In [17] the author presents security architecture for mobile wireless sensor nodes by using a cryptographic algorithm. This algorithm proposes an authentication mechanism between the sensor nodes which provides security only form external threats.

The authors proposed a protocol called BROadcast Session Key Negotiation Protocol (BROSK) in [18]. This BROSK protocol uses broadcasting key negotiation massage to provide link dependent keys to the sensor nodes for communication. This scheme uses simultaneous transmission for communication that increases the rate of collision.

In [19] the author proposed key distribution scheme using tree based approach in Wireless Sensor Network (WSN). They discussed scenario of sharing key when a new sensor node joins a network and assume to share its key with its neighbour. The proposed scheme is complex in nature and need extra computation resources. In [20] the authors have provided a framework for security with three management schemes for WSN. They evaluate these schemes on WSN challenging issues such as memory constraints, energy utilization, communication patterns, scalability, connectivity and communication patterns. The authors evaluate SACK, SACK-P and SACK-H management keys. The result shows that there exists inverse relationship between security and available resource utilization.

The above discussed security techniques such as encryption and authentication are not best suited in WSN environment. Therefore, there is a need for dynamic security mechanism in WSN. Intrusion Detection System (IDS) provides the dynamic security mechanism to WSN. We have surveyed several research articles in which variety of IDS are installed on WSN. Let's have a look at some of these techniques.

In [21] the authors have differentiated the available securities models. Currently two types of models are used for security: Intrusion Prevention (IP) and Intrusion detection (ID). IP uses authentication and firewalls for securing the boundaries of the network and ID uses some detection mechanism for identifying the intrusion in the networks. In [22] the authors notify the difference between IDS approaches for identifying and deflecting attacks. Host-based and Network-based are two types of approaches used by IDS. The authors highlighted the strengths and weakness of each approach. They argued that both of these techniques work together for achieving better intrusion detection and prevention.

Whereas in [23] the authors proposed a distributed intrusion detection scheme to monitor neighbour nodes for bringing the network back to function. They assume that adversary cannot capture or introduce new nodes inside the network. The proposed scheme creates a trust relation on neighbouring nodes which is not suitable if the trusted node is under attack.

Whereas, in [24] the authors have introduced a technique that observes the neighbourhood node communication called the spontaneous watchdog. The authors assume that the sensor nodes are stationary and used MICA2 radio stack for energy consumption. The decision for the selection of spontaneous watchdog imposed workload on the nodes and extra energy is required for activating global agent is the major drawback of this technique. In addition, the nodes are independent which do not assure only one global agent is activated per packet in the network.

The bottom-line is that, in existing IDS schemes in WSN, there seems an inverse relationship between enhanced security and efficient resource utilization in WSN. We need a better security mechanism which optimally utilize the resources of the WSN and provides better level of overall security.

3. Proposed Scheme

We have proposed a Mobile Agent Based Hierarchical Intrusion Detection System (MABHIDS) that provide two tiers of security in WSN. In this portion, we will discuss the architecture and working paradigm of proposed scheme in Section A and Section B respectively.

3.1 Architecture

In order to provide two tiers of security we have installed Musk architecture [25] on each Cluster Head (CH). We have modified the MUSK architecture in order to behave as mobile agent. This architecture works as the Network Intrusion Detection System (NIDS) as well as Local

Intrusion Detection System (LIDS) on WSN. We have used two threshold frequencies. The threshold 1 is set on each CH for the normal activity of the network and threshold 2 is set on each sensor node for its normal activity.

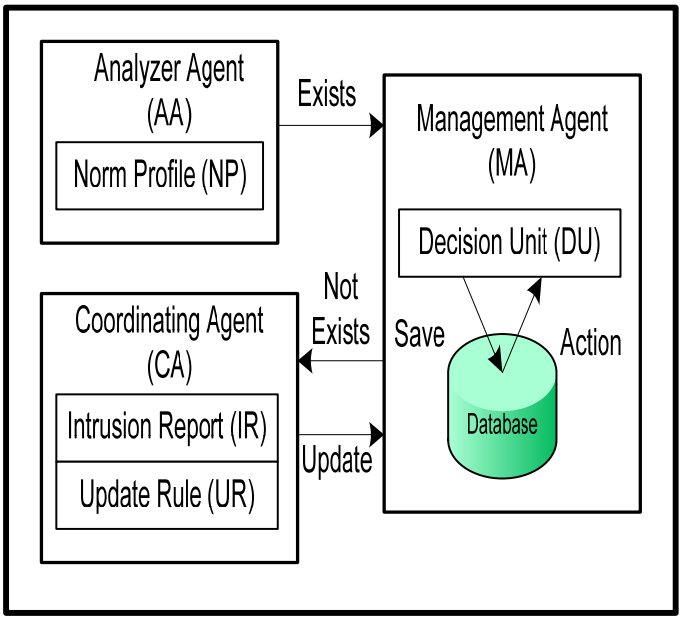

Fig. 2 MUSK Architecture [25]

NIDS: The different agents of Musk architecture [25] works as NIDS which is installed on each Cluster Head (CH) within a network. The NIDS capture the data packets along the path to identify an intrusion activity. The modified form of Musk architecture is shown in the Fig.2. This architecture is comprises of three agents: Analyzer Agent (AA), Coordinating Agent (CA) and Management Agent (MA). When the CH detects an intrusion it sends a copy of Analyzer agent (AA) to the victim node. Therefore AA is mobile in nature. The CA and MA are preset in the CH and they are fixed.

Analyzer Agent (AA): The Analyzer Agent (AA) is used to monitor node activity. It is a mobile agent and installed on each CH in the network. When CH discovers an intrusion it sends a copy of AA to the suspicious node. The AA uses victim resources in order to verify the occurrences of intrusion. The AA generates a Norm Profile (NP) and check the threshold 2. If there is a deviation from the threshold frequency the AA generates an alarm and notifies the CH. The CH calls the Management Agent (MA) for analysis.

Management Agent (MA): The Management Agent (MA) contains a sub unit called Decision Unit (DU) for the analysis of intrusion. The DU maintains the database of already occurred intrusions. When an intrusion occurs the CH calls the MA for analysis. The MA activates its DU that searches in its database whether this intrusion happens in the past or not. The database contains the predefined stored intrusions along with the decisions. If the match occurs against the pre stored intrusions then DU performs already stored decision and informs to the CH. If there is no such entry in the database then MA informs the Co-ordinating Agent (CA) regarding the occurrence of novel intrusion.

Coordinating Agent (CA): The Coordinating Agent (CA) performs two basic functions i.e. generate Intrusion Report (IR) and Update Rule (UR). When CA receives a novel intrusion message from MA it sends to IR. The IR forwards this report to the Base Station (BS) regarding the occurrence of intrusion. The BS is a centralized decision making authority against the intrusion. It makes a decision on novel intrusion and sends it to the Update Unit (UU). The UU generates new rule against that intrusion and send it to MA. The MA saves the intrusion in the database for future use. If the same intrusion happens again the DU searches the database and performs the already stored decision.

LIDS: The Analyzer Agent (AA) is a mobile agent and works as LIDS. When NIDS in CH deviate from its threshold 1 it generate an alarm informing the occurrence of intrusion. The CH makes analysis and identifies the sensor node that is generating abnormal traffic. The CH activates its mobile AA and send to the victim node. The AA works as LIDS and uses resources of the suspicious node for identifying the malicious activities. The AA informs the CH either the suspicious node is victim or safe. If the node is victim the CH that takes appropriate action upon that activity. The copy of AA is only send to the suspicious node instead of installing LIDS on each sensor node.

The fig-3 is representing a working deployment of NIDS & LIDS. It is vital to mention here that the NIDS is deployed on each CH whereas the actual deployment of LIDS is also at CH. On each intrusion alarm, the LIDS (which are a mobile agent) are triggered by CH for further inspection of the behaviour of suspicious node. The LIDS uses resources of suspicious node to report it either as a victim or safe node.

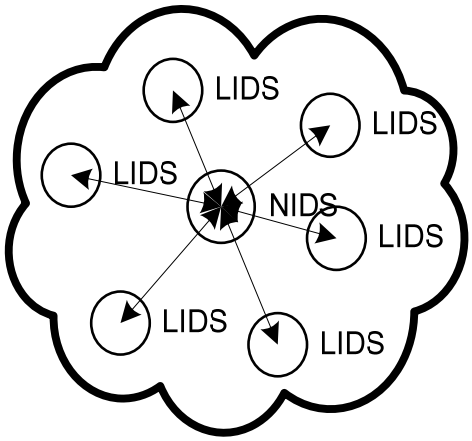

Fig. 3 Working Deployment of NIDS & LIDS.

3.2 Working Paradigm

We set two threshold levels for intrusion detection, one for Network Intrusion Detection System (NIDS) and other for Local Intrusion Detection System (LIDS). Threshold 1 is set on each CH over the network and works as the NIDS whereas; the threshold 2 is set on each sensor node and works as LIDS. The initial intrusion detection is performed by NIDS which detects the normal rate of packet arrival and departure. In case of deviation from threshold 1, the CH triggers the mobile Analyzer Agent (AA) over the link where deviation is occurred.

The AA will visit the suspicious node and acts as Local Intrusion Detector (LID) over there. The AA will use the resources of suspicious node to investigate its behaviour further. This investigation is based on threshold 2. If suspicious node is found the victim the AA will update CH. The CH inform its sub agents i.e. Coordinating Agent (CA) and Management Agent (MA) that will take appropriate action to prevent rest of the network from intrusion either by minimizing the communication with the victim node, reducing the trust value on the victim node or by cutting its communication from rest of the network. Otherwise, the AA informs the CH that the suspicious node is not the victim; it is a safe node and unusual but harmless activity has taken place.

4. Advantages

The Major advantage our proposed approach is that it provides two levels of security by using resources of sensor network optimally. It also reduces the workload of Cluster Head (CH) and provides enhanced security. As in existing schemes CH is responsible for all computation pertaining to the intrusion detection activity in member nodes of the CH. Whereas in our proposed scheme CH triggers the AA for suspicious node on its every unusual activity. The AA uses suspicious node's resources in order to declare it either as a victim or safe node. In this way CH resources are saved as compare to the existing schemes. Another benefit of our approach is infrastructural reduction as we do not need to install LIDS on every node rather mobile agent acts as a LIDS on suspicious node. This enhances the overall life time of the sensor network.

5. Performance Evaluation

We have performed the analytical performance comparison of our proposed scheme with existing schemes. We analyzed their performance on two major factors i.e. Security and Efficiency.

The security factor is divided further into three parameters i.e. internal external and novel threats. Internal threats are those attacks that are initiated or injected by the intruder residing inside the network. External threats are from outside attackers. Novel threats are the unusual or unrecognized form of the intrusions which have not occurred previously. Three types of possible values used by these intrusions are low, high and medium that indicates how clearly the proposed scheme identifies these intrusions. We have given the low value to all those schemes that doesn't provide defence against the compromised node, under attack nodes, inside attackers, master or secret key is captured or the node activity is dependent on the neighbourhood node information, trust relationship on nodes etc. the medium value to the all those proposed scheme that identify the intrusion but does not provide any defensive measurement how to handle them, generate false negative in large amount. The high value to all those schemes that clearly identify the intrusion as well as provide the counter measure against that intrusion, compromise of one node will not make the whole security of the system vulnerable.

We divide the efficiency factor into three parameters i.e. computation costs, network bandwidth, node resource utilization and number of messages. Two types of values are used high and medium in computation cost, network bandwidth and node resource utilization. We have given high value to all those schemes that increases burden on network resource i.e. cryptographic algorithms are resource hungry in nature that require extra computation and memory overhead, communication steps between nodes increases, simultaneous transmission increases the rate of collision that effect the bandwidth issues, large amount of false negative dissipate the energy resources etc. The medium value is given to the scheme that uses victim resources in order to discover an intrusion by using minimum network resources. The number of messages which contains the integer value i.e. additional steps used by the proposed schemes in order to identify the intrusion. Table 1 shows that our proposed

scheme is efficient in several aspects as compare to the existing schemes

Table 1: Performance comparison between different existing schemes

Sr. No	Scheme Name	Security			Efficiency			
		Internal Threats	External Threats	Novel Threats	Comp. Costs	Network Band-Width	Node Resource	No. of Messages
1	Security Protocol for Sensor Networks [16]	Low	High	Low	High	High	High	8
2	A Security Architecture for Mobile WSN [17]	Low	High	Low	High	High	High	---
3	Scalable Session Key Construction Protocol for WSN [18]	Low	Low	Low	High	Medium	High	---
4	A Tree Based Approach for Secure Key Distribution in WSN [19]	---	---	---	High	Medium	High	4+4
5	A unified security framework with three key management schemes for WSN [20]	Low	High	Low	High	High	High	---
6	A Decentralized IDS for Increasing Security of WSN [26]	High	High	High	High	High	High	---
7	An IDS for WSN [27]	Medium	Medium	High	---	High	High	---
8	Anomaly Intrusion Detection in WSN [28]	Medium	Medium	---	---	---	---	---
9	Decentralized Intrusion Detection in WSN [29]	---	---	---	High	High	High	---
10	Intrusion Detection based Security Architecture for WSN [30]	Medium	Medium	High	High		High	---
11	Energy Efficiency of IDS in WSN [31]	High	High	High	High	High	High	---
12	An Improved IDS Based On Agent [32]	---	---	---	High	High	High	---
13	A Framework of Machine Learning Based Intrusion Detection for WSN [33]	---	---	Low	---	---	High	---
14	Mobile Agent Based Hierarchical IDS (Proposed Scheme)	High	High	High	Medium	Medium	Medium	---

6. Conclusions

The resource restricted nature of WSN demands a more sophisticated and secure security mechanism for these sorts of networks. There seems an inverse relationship in better security and optimum resource utilization of network resources in existing security schemes of WSN. In this research article, we have proposed a security model which not only provides good level of security but it also uses network resources optimally for the provision of better security. In proposed approach, we have proposed a two tier security model for WSN. The NIDS and LIDS are involved in providing two tier securities. The NIDS is installed on all CH whereas LIDS is based on mobile agent. The LIDS is activated whenever CH found any node suspicious. The CH issues LIDS for further scrutiny of malicious activities of suspicious node in order to affirm it as a compromised node. The LIDS uses resources of suspicious node. The proposed mechanism provides enhanced security using resources of WSN optimally. The workload of CH is also reduced using our proposed. Our proposed approach also helps in security infrastructural reduction for enhanced security.

References

[1] S. Kaplantzis, “Security Models for Wireless Sensor Networks”, Research Thesis, 2006.
[2] A. Perrig, J. Stankovic and D. Wagner, “security in wireless sensor networks” communications of the ACM, vol. 47, no. 6, June 2004.
[3] D. Culler, “Overview of sensor Networks” University of California, Berkeley Deborah Estrin Mani Srivastava University of California, Los Angeles, IEEE Computer society, August 2004.
[4] A. Bob, “What is sensor network” National Instruments, LabVIEW, NI, White Paper.
[5] F.L. Lewis, “Wireless Sensor Networks” Smart Environments: Technologies, Protocols, and Applications Conference, New York, 2004.

[6] S. Ramesh, "A Protocol Architecture for Wireless Sensor Networks" School of Computing, University of Utah, 2006.
[7] Y. Wang, G. Attebury, and B. Ramamurthy, "A survey of security issues in wireless sensor networks" University of nebraska-lincoln, IEEE Communications Surveys & Tutorials, 2006.
[8] M. Sharifnejad, M. Sharifi, M. Ghiasabadi and S. Beheshti, "A survey on wireless sensor networks security" published in 4th international conference: sciences of electronic, technologies of information and telecommunications, Tunisia, 2007.
[9] A.D. Wood and J.A. Stankovic, "Denial of Service in Sensor Networks", University of Virginia, IEEE Conference, 2002.
[10] C-Y. Chong and S. P. Kumar, "Sensor Networks: Evolution, Opportunities, and Challenges" proceedings of the IEEE, vol. 91, no. 8, August, 2003.
[11] A. Perrig, J. Stankovic, and D. Wagner, "Security In Wireless Sensor Networks", communications of the ACM, vol. 47, no. 6, June 2004.
[12] Y. Wei, L. Paul and J.M. Havinga, "How to Secure a Wireless Sensor Network", Faculty of Electrical Engineering, Mathematics and Computer Science, University of Twente, Netherlands, Published by IEEE ISSNIP, 2005.
[13] T. Zia and A. Zomaya, "Security Issues in Wireless Sensor Networks" School of Information Technologies, University of Sydney, Published by IEEE, 2007.
[14] R. Omer, O. Kasten and F. Mattern, "Middleware Challenges for Wireless Sensor Networks", Department of Computer Science, ETH Zurich, Switzerland, Mobile Computing and Communications Review, Volume 6, Number 2, 2004
[15] R. Roman1, J. Zhou, and J. Lopez, "On the Security of Wireless Sensor Networks", Institute for Infocomm Research, Heng Mui Keng Terrace, Singapore and Ingenieria Informatica, University of Malaga, Malaga, Spain, 2005.
[16] A. Perrig, R. Szewczyk, J.D. Tygar, Victorwen and E. Culler, "SPINS: Security Protocols for Sensor Networks" Department of Electrical Engineering and Computer Sciences, University of California, Berkeley, Wireless Networks, 2002.
[17] S. Schmidt, H. Krahn, S. Fischer, and D. Watjen "A Security Architecture for Mobile Wireless Sensor Networks" by Springer-Verlag Berlin Heidelberg, LNCS, 2005.
[18] B. Lai, S. Kim and I. Verbauwhede, "Scalable Session Key Construction Protocol for Wireless Sensor Networks", Department of Electrical Engineering University of California, Los Angeles, USA, 2003.
[19] E. Blaß, M. Conrad and M. Zitterbart, "A TreeBased Approach for Secure Key Distribution in Wireless Sensor Networks.", 2006.
[20] R. Riaz, A. Naureen, A. Akram, A.H. Akbar, K.H. Kim, H. F. Ahmed "A Unified Security Framework With Three Key Management Schemes For Wireless Sensor Networks", Elsevier, 17 June 2008.
[21] J. G. Tront and R. C. Marchany, "Internet Security: Intrusion Detection & Prevention", IEEE Proceedings of the 37th Hawaii International Conference on System Sciences, 2004.
[22] A. Bob, "Network- vs. Host-based Intrusion Detection" A Guide to Intrusion Detection Technology, ISS Internet Security System October 2, 1998
[23] K. Ioannis, T. Dimitriou and F. Freiling, "Towards Intrusion Detection in Wireless Sensor Networks" Athens Information Technology, 19002 Peania, Athens, Greece and Department of Computer Science, University of Mannheim, Germany, 2006
[24] R. Roman, J. Zhou and J. Lopez, "Applying Intrusion Detection Systems to Wireless Sensor Networks", Communications Society publication in the IEEE CCNC 2006.
[25] S. Khanum, M. Usman, K. Hussain, R. Zafar, and Dr M. Sher, "Energy-Efficient Intrusion Detection System for Wireless Sensor Network Based on MUSK Architecture" HPCA 2009, LNCS 5938, pp. 212–217, Springer-Verlag Berlin Heidelberg 2010
[26] I. Chatzigiannakis and A. Strikos, "A Decentralized Intrusion Detection System for Increasing Security of Wireless Sensor Networks",2005.
[27] I. Onat and A. Miri, "An Intrusion Detection System for Wireless Sensor Networks", published by IEEE, 2000.
[28] V. Bhuse and A. Gupta, "Anomaly Intrusion Detection in Wireless Sensor Networks", Western Michigan University, Kalamazoo, USA, 2005.
[29] Ana Paula et. al., "Decentralized Intrusion Detection in Wireless Sensor Networks", ACM, 2005.
[30] D. Xiao, C. Chen and Gaolin Chen, "Intrusion Detection based Security Architecture for Wireless Sensor Networks", IEEE, 2005.
[31] P. Techateerawat and A. Jennings, "Energy Efficiency of Intrusion Detection Systems in Wireless Sensor Networks", IEEE, 2006.
[32] B. Dong and X-L. Liu, "An Improved Intrusion Detection System Based On Agent", IEEE, 2007.
[33] Z. Yu and J.P. Tsai, "A Framework of Machine Learning Based Intrusion Detection for Wireless Sensor Networks" Department of Computer Science, University of Illinois at Chicago, IEEE, 2008.

Authors:

Surraya Khanum is M.Phil / MS in computer science with the specialization of Computer Networks. She has numerous international publications in the area of network security. Currently she is working as a Lecturer in Computer Science in Faculty of Computer Science, King Khalid University, Abha, Kingdom of Saudi Arabia. Her research interests include networks, network security, wireless networks, sensor networks and intrusion detection systems.

Muhammad Usman is M.Phil / MS in Computer Science with specialization in Computer Networks. He is scholarship holder to undertake his PhD studies from Griffith University, Australia from Feb, 2012 to Jan 2015. He has 8 years of teaching, research and professional experience. Currently he is working as a Lecturer in Computer Science in King Khalid University, Abha, Kingdom of Saudi Arabia. He has several international publications. His research interest includes networks, network security, wireless networks, mobile ADHOC networks, wireless sensor networks, intrusion detection systems and ongoing issues in multimedia.

Ala'a A. Alwabel is MS in Information System with the specialization of information security. She has International publication in the area of Information Security. Currently she is working as a coordinator and lecturer in Faculty of Computer Science, department of Information System, King Khalid University, Abha, Kingdom of Saudi Arabia. Her research interests include Wireless Networks, Networks Security, Cryptography, Information Security, Information Retrieval and E-Health.