Current Trends in Technology and Science
ISSN: 2279- 0535. Volume: 3, Issue: 4(June-July 2014)

False Misbehavior Removal in Clonal Selection Mechanism Based on Watchdog by the use of Transition Point in a Wireless Sensor Network

Phiza Ambreen Khan
Research Scholar, Department of CSE (Software Engineering), SSSIST,Sehore, M.P., India, fiza9387@gmail.com

Kailash K. Patidar
Assistant Professor, Department of CSE (Software Engineering), SSSIST, Sehore, M.P., India,

Gajendra Singh
Professor & Head, Department of CSE (Software Engineering), SSSIST,Sehore, M.P., India, gajendrasingh@gmail.com

Mukesh Tiwari
Dean Academic, SSSIST, Sehore, M.P., India,

Abstract — A wireless sensor network is a network consisting of number of wireless sensors, also called as node, which cooperate each other in sensing some sort of physical characteristics or general environmental conditions, such as temperature, sound, vibrations, light, movement etc. These networks can consist of everything from smaller number of nodes for sparsely populated networks, up to 100's of thousands of nodes in densely populated networks. Watchdog algorithm is in existence is unable to catch the misbehaving sensors due to which network traffic is being upset. Our goal is to create an IDS such that the throughput of the system must be efficiently increased and PDR must be improved. The constraint of the system with our protection scheme must be comparable with the system without having any attack. We implement two algorithms simultaneously to detect the nodes which acting as true node and fake other true nodes to be misbehaving. We implement this approach in the watchdog mechanism to improve the performance, throughput, accuracy, energy efficiency at low cost and less time consuming.

Keyword — Wireless Sensor Network, Security Goal, False misbehavior, Numbering, Energy Consumption, Watchdog, IDS

1. INTRODUCTION

A wireless sensor network is a network [1] consisting of number of wireless sensors, also called as node, which cooperate each other in sensing some sort of physical characteristics or general environmental conditions, such as temperature, sound, vibrations, light, movement etc. These networks can consist of everything from smaller number of nodes for sparsely populated networks, up to 100's of thousands of nodes in densely populated networks. The individual sensor nodes are relatively small and have limited amount of energy, computational power and memory. For this reason they are well suited to a substantial amount of monitoring and surveillance applications. Popular wireless sensor network applications include wildlife monitoring, bushfire response, military command, intelligent communications, industrial quality control, observation of critical infrastructures, smart buildings, distributed robotics, traffic monitoring, examining human heart rates etc. Majority of the sensor network are deployed in hostile environments with active intelligent opposition. Hence security is a crucial issue. One obvious example is battlefield applications where there is a pressing need for secrecy of location and resistance to subversion and destruction of the network. Majority of the sensor network are deployed in unreceptive environments with active intelligent opponent. Hence security is a crucial issue. The nodes in network are performing routing independent but the whole activity of nodes is watch by Base Station (BS). Less obvious but just as important security dependent applications [2, 3, 4] include:

- *Disasters:* In many disaster scenarios, especially those induced by terrorist activities, it may be necessary to protect the location of casualties from unauthorized disclosure
- *Public Safety:* In applications where chemical, biological or other environmental threats are monitored, it is vital that the availability of the network is never threatened. Attacks causing false alarms may lead to panic responses or even worse total disregard for the signals.
- Home Healthcare: In such applications, privacy protection is essential. Only authorized users should be able to query and monitor the network.

Basically attacks are classified into two types: Active attacks and Passive. False misbehavior Attack is active in nature. A malicious node purposely reports that other nodes are misbehaving. A sensor node which is malicious in nature can report that some other true node

Copyright © 2014 CTTS.IN, All right reserved

is dropping packets while other node is not. In this case the neighbor nodes which cannot communicate directly to each other can think true nodes as malicious. In Dissertation, our work is to prevent the network from false misbehavior Attack.

The major contribution of this paper includes classification of security attacks in Wireless Sensor Networks in Section 2 and Section 3 gives the detailed information about Related Work that has been done in this field. Section 4 has explained the problem statement and Criteria of Attack Detection has discussed in section 5. Section 6 has provides the information of Simulation Environment and Results and at last the final conclusion of paper are mentioned in Section 7.

2. ATTACKS ON SENSOR NETWORK

Wireless Sensor networks are vulnerable to security attacks [5, 6] due to the broadcast nature of the transmission medium. Furthermore, wireless sensor networks have an additional vulnerability because nodes are often placed in a hostile or dangerous environment where they are not physically protected. Basically attacks are classified as active attacks and passive attacks.

1. Passive Attacks

The monitoring and listening of the communication channel by unauthorized attackers are known as passive attack. The Attacks against privacy is passive in nature.

• *Attacks against Privacy*

The main privacy problem is not that sensor networks enable the collection of information. In fact, much information from sensor networks could probably be collected through direct site surveillance. Rather, sensor networks intensify the privacy problem because they make large volumes of information easily available through remote access. Hence, adversaries need not be physically present to maintain surveillance. They can gather information at low-risk in anonymous manner. Some of the more common attacks [8] against sensor privacy are:

• *Monitor and Eavesdropping:* This is the most common attack to privacy. By snooping to the data, the adversary could easily discover the communication contents. When the traffic conveys the control information about the sensor network configuration, which contains potentially more detailed information than accessible through the location server, the eavesdropping can act effectively against the privacy protection.

2. Active Attacks

The unauthorized attackers monitors, listens to and modifies the data stream in the communication channel are known as active attack. The following attacks are active in nature.

1. Routing Attacks in Sensor Networks
2. Distributed Denial of Service Attacks

3. RELATED WORK

Shield, the existence of effective filtering and attack filtering systems and deals with the deployment problem. Since Shield is deployed between two routers and blocks out traffic passing between the two routers, they needed to deploy several Shields and tried to optimize the number and location of Shields. Lastly, to efficiently manage the system, this work systematized Shied to operate in three phases by the riskiness of attacks.

Forootaninia[1] et.al proposed "An Improved Watchdog Technique based on Power-Aware Hierarchical Design for IDS in Wireless Sensor Networks", they focused on to resolve the ambiguous collision of packets in watchdog mechanism. There are certain problems existing in watchdog have been resolved but still one of the problems in watchdog, the malicious node detection due to ambiguous collision of packets has not been solved.

Youngho Cho[2] et.al proposed " Insider Threats against Trust Mechanism with Watchdog and Defending Approaches in Wireless Sensor Networks", they focused on overhearing ability of the sender sensor node within its transceiver range But watchdog has the limitation of not being able to detect the misbehaving nodes in the following conditions.

Yuxin Mao[3] et.al proposed "A Secure Mechanism for Data Collection in Wireless Sensor Networks", the objective is to improve the existing watchdog monitoring system by implementing the change point detection algorithm in it, there by detecting the exact malicious node in the network.

Lei Huang [4] et.al proposed Extended Watchdog Mechanism for Wireless Sensor", they focused on to overcome the limitations of watchdog monitoring system which was improved by adding a threshold mechanism .In this mechanism sensor node stores all recently sent packets in its buffer, and compares each packet with the overheard packet to see whether there is a match.

Abror Abduvaliyev [5] et.al proposed "On the Vital Areas of Intrusion Detection Systems in Wireless Sensor Networks", in this mechanism signal strength was proposed to detect the malicious nodes in a network. The idea was to compare the signal strength of reception with its expected value. A signal is only detected by a receiving node if the received signal power is equal or greater than the received signal power threshold. If the signal power received is less than the threshold then the particular node is suspected to be malicious.

CE Loo[6] et.al proposed "Intrusion Detection for Routing Attacks in Sensor Networks", The detecting technology and sensing technology combined with processing power and wireless communication makes it lucrative for being adopted in great quantity in future. The wireless communication technology is also looking for various types of security threats.

Sergio[7] et.al proposed "Mitigating routing misbehavior in mobile adhoc networks", they focused on to design routing protocol for WSN is very much challenging

Copyright © 2014 CTTS.IN, All right reserved

manner and shows that the protocols have a high diversity to match up with requirements of the application scenarios.

A. Babu[8] et.al proposed "False Misbehavior Elimination In Watchdog Monitoring System Using Change Point In A Wireless Sensor Network", they focused on both the possibilities of detecting the malicious node and also declaring a true node to be malicious. By using the proposed algorithm the exact malicious node is found to be identified in all the rounds. The malicious node detected by the proposed algorithm is found to be accurate irrespective of the number of rounds conducted.

4. PROBLEM STATEMENT

We assume that a WSN contains one BS and a large number of sensor nodes, organized in a tree-type topology. Each sensor node has limited resources of power, memory, processing and communication capabilities and functions in unattended manner. All sensor nodes monitor the environment and send sensed data periodically in a hop-by-hop manner towards the BS using the same radio channel. The objective is to improve the existing watchdog monitoring system based on clonal selection algorithm by implementing the transition point detection algorithm in it, thereby detecting the exact malicious node in the network.

5. PROPOSED APPROACH

Proposed Algorithm for malicious node detection and false behavior elimination in WSN:

Input: T =A topology in which m number of malicious node present in a set of n number of sensor nodes.
Output: O = set of clusters which are having watchdog nodes used to find malicious nodes Set initial parameter of network

Step 1: Mobile Sensor Node's = N;
MAC layer = 802.11
Routing = AODV
Attacker nodes = False Misbehavior
Provide Security = PSF (Protection scheme for false misbehavior)
Inter Arrival Time = IAT (Control Rate at Different Time)
//Attacker launches false misbehavior
Attacker-node (capture vulnerable node information && send =false alarm packet && rate = 2^{32}*0.1s)
If (Sink detects a discontinuous sequential number)
{
Infected;
Broadcasts an alert packet;
}
Step 2 : For (Intermediate node check for the missing sequence in its cache)
{
If
{
Missing packet found;
Send back to the node;
}
Else
{
Sends back a normal response packet;
}
}
Step 3 :If (Sink receive number of response packets)
{
Intermediate node does not send any response, its identity recorded;
}
Step 4 : Generate trace file for further analysis

Step 5 : Do (analysis trace for detection)
{
Analyze the nodes of the routing path, Mark the malicious node;
Find infection ratio;
}
Step 6: Call protector PSF
While (PSF-Check vulnerable node && total packet receives && rate && sender)
{
For (S_i Watches Si+1 whether data sent successfully or not)
{
At the same time S_0 sends the data to the Si;
If
{
S_{i+1} is a true node;
Response bit of S_i is zero;}
Else
Response bit of Si can send zero or one;
}
Step 7 : Do (When it reaches S_n all the response bit will be
send to the S_k)
{
Suspicious point = previous status bit as 0 or -1 transit to 1;
Mark the suspicious node and Block the malicious
node;
}

6. CRITERIA FOR ATTACK DETECTION

Sensor nodes monitor the environment and transmit the acquired data in a hop-by-hop manner to a sink node. The Receiver got the intermediate nodes response packet. It further examines them for confirmation and validation. Let an assumption is made that the status bit value for a negative packet is 1 and status bit value positive packet is

Copyright © 2014 CTTS.IN, All right reserved

0. The node which does not responded has status bit value set to be -1. All the nodes having -1 status bit value are placed in a set considered as suspicious nodes. These nodes are still not marked as malicious; there may be some other reasons of getting no response i.e. interference or low transmission power. The receiver assembles the status bit in subsequent packet transmissions. If a node having previous status bit 0 or -1 and in subsequent data collection its value transit to 1 that point is considered as suspicious point. The found as suspicious long with upstream and downstream nodes create a malicious sequence. We implement this approach in the watchdog mechanism to improve the performance, throughput, accuracy, energy efficiency at low cost and less time consuming.

7. Simulation Environment and Results

The simulation is implemented In Network Simulator 2.31 [16], a simulator for mobile ad hoc networks. The simulation parameters are provided in Table 1. We implement the random waypoint movement model for the simulation, in which a node starts at a random position, the simulation time is 100, and then moves to another random position with a velocity chosen random and maximum up to 30 m/s. A packet size of 512 bytes and a transmission rate of 4 packets /s.

TABLE I. Simulation Parameters for Case Study

Examined Protocol	AODV
Number of nodes	100
Dimension of simulated area	800×600
Simulation time (seconds)	50
Radio range	550
Traffic type	CBR, 3pkts/s
Packet size (bytes)	512
Number of traffic connections	TCP/UDP
Maximum Speed (m/s)	30
Node movement	Static
Types of attack	False misbehaviour
Attacker Nodes	5
Watcher node	5

Performance Metrics:

In our simulations we use several performance metrics to compare the proposed AODV protocol with the existing one. The following metrics were considered for the comparison were

- *Throughput:* Number of packets sends in per unit of time.
- *Packet delivery fraction (PDF):* The ratio between the numbers of packets sends by source nodes to the number of packets correctly received by the corresponding destination nodes.
- *End to End delay*: Measure as the average end to end latency of data packets.
- *Normalized routing load:* Measured as the number of routing packets transmitted for each data packet delivered at the destination.

Simulation Results

In this segment the analysis of simulation outcome are mentioned with the situation of normal routing, in case of intrusion and with secure IDS scheme.

PDF Analysis

PDF is the ratio of packets received by send. The PDF in case of attack are only evaluated at time 35 seconds but after applying security scheme PDF is improved and equal to normal. While in case of attack PDF is clearly very low. The protection scheme enhanced the performance and provides the competent PDR in system.

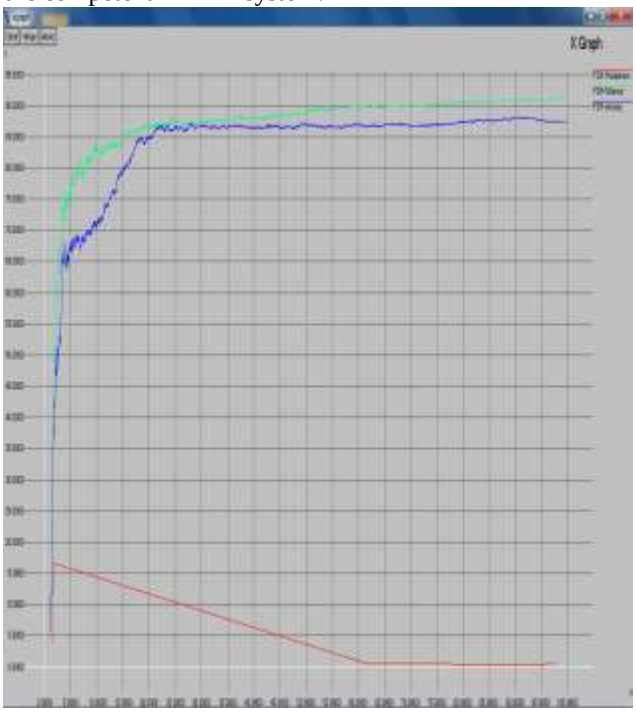

Fig. 1.PDF analysis

Routing Load Analysis

The false misbehaving nodes behave as optimal path and report other nodes as malicious nodes. It captures all the traffic and blocks the other routes. Therefore in case of attack routing load is comparatively low. After implementing the protection scheme routing load is increased and comparable with normal routing behaviour.

Copyright © 2014 CTTS.IN, All right reserved

Current Trends in Technology and Science
ISSN: 2279- 0535. Volume: 3, Issue: 4(June-July 2014)

Fig. 2.Routing load analysis

Throughput analysis

This graph shows the throughput study in case of normal routing, presence of intruder and protected environment. The throughput is calculated as number of data packets are received at sink in per second. In the presence of attack, throughput decreases because of dropped packets by the attacker nodes. It is measured only up to 35 seconds in network. But after applying protection scheme the throughput is increased.

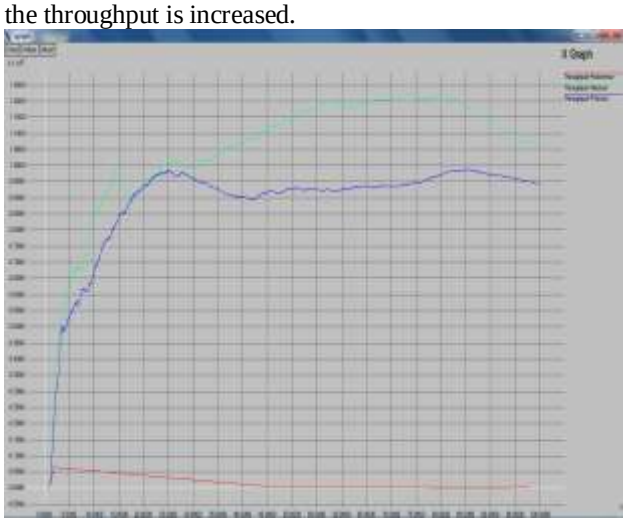

Fig. 3.Throughput Analysis

Infection analysis

This graph represents the infection percentage analysis in case of attack. Here we clearly view high percentage of infection in case of attack. But after applying protection scheme the infection are zero in presence of attack it means, the security scheme are totally block the misbehavior movement of attackers and at the end intruder are not show infection

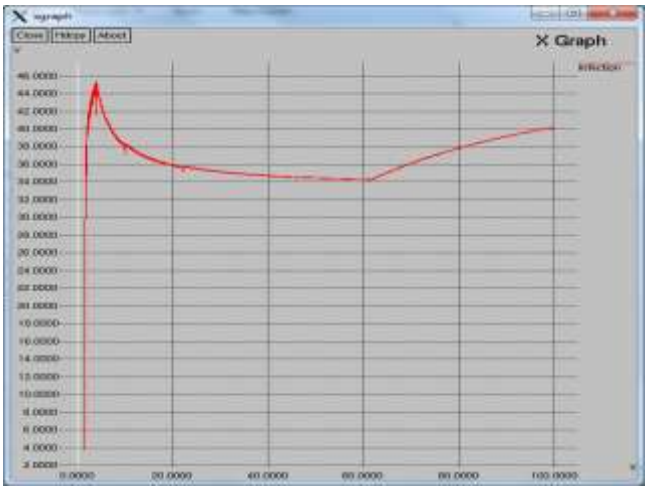

Fig. 4. Infection analysis

8. Overall Analysis

The overall performance of network is shown in table 2. This table shows the whole summery of performance metrics in exact numeral form means how many packets are sent, received and lost so on in WSN in case of normal routing, attack and IDS. The protection scheme provides the normal behavior in presence of attacker.

TABLE II. Overall summery of Performance Metrics

Performance Parameters	Normal Routing	Attack Case	IPS-Case
SEND	6637	2022	6139
RECV	6048	9.00	5358
ROUTINGPKT	12391	2327	12984
PDF	91.13	0.45	87.28
NRL	2.05	258.56	2.42
DROPRTS	1978	501	25987
No. of dropped data (packets)	589	2013	781

9. Conclusion

In WSN the nodes are constantly exchanging the information in network. But the data is lost because of attack and routing overhead stopped. All the data select the path containing attacker nodes. The planned mechanism removes the need for a centralized authority which is not practical in wireless sensor network because of their self organizing nature.

The results demonstrate that the presence of a false misbehaving node increases the packet loss and decrease throughput in the network significantly. The proposed mechanism secures the network through a self organized, fully distributed and localized procedure. The attacker has infected the 42% network performance in network but because of that remaining performance of network is also affected. The major benefit of this scheme is the scheme are provides the 100% performance if compare to normal routing behavior of

Copyright © 2014 CTTS.IN, All right reserved

network. The security scheme showing the better results in presence of attacker.

In future, we analyze the behavior of other attacks like Black hole attack, Wormhole attack and try to implement the security scheme and compare the performance ratio for that attack.

REFERENCES

[1] An Improved Watchdog Technique based on Power-Aware Hierarchical Design for IDS in Wireless Sensor Networks A. Forootaninia1 and M. B. Ghaznavi-Ghoushchi,International Journal of Network Security & Its Applications (IJNSA), 2012

[2] Insider Threats against Trust Mechanism with Watchdog and Defending Approaches in Wireless Sensor Networks Youngho Cho and Gang Qu, IEEE Symposium on Security and Privacy Workshops ,2012

[3] A Secure Mechanism for Data Collection in Wireles Sensor Networks Yuxin Mao, School of Computer and Information Engineering, Zhejiang Gongshang University,Applied Mathematics & Information Sciences – An International Journal, 2010.

[4] Extended Watchdog Mechanism for Wireless Sensor Networks Lei Huang +, Lixiang Liu, Journal of Information and Computing Science, 2007

[5] Abror Abduvaliyev, Al-Sakib Khan Pathan, "On the Vital Areas of Intrusion Detection Systems in Wireless Sensor Networks" in IEEE Communications Surveys & Tutorials,Vol. 15, No. 3, Third Quarter 2013

[6] CE. Loo, MY. Ng, C. Leckie, and M. Palaniswami, Intrusion Detection for Routing Attacks in Sensor Networks,International Journal of Distributed Sensor Networks, vol. 2,pp. 313-332, 2006.

[7] Sergio Marti, T. J. Giuli, Kevin Lai, "Mitigating routing misbehavior in mobile adhoc networks" in MobiCom '00: Proceedings of the 6th annual international conference on Mobile computing and networking, pages 255–265, New York, NY, USA, 2000. ACM.

[8] A.Babu Karuppiah, T.Meenakshi, "False Misbehaviour Elimination In Watchdog Monitoring System Using Change Point In A Wireless Sensor Network" in International Journal of Graduate Research in Engineering and Technology (GRET),2012.

[9] Tapas Badal and Dipti Verma, "A Modular Approach for Intrusion Detection System in Wireless Networks", International Journal of Advances in Computer Networks and Security, pp. 57-61, May 2012.

[10] Chilakalapudi Meher Babu, Dr. Ujwal A. Lanjewar, Chinta Naga Manisha "Network Intrusion Detection System on Wire Less Mobile Ad hoc Networks" International Journal of Advanced Research in Computer and Communication Engineering Vol. 2, Issue 3, pp. 1495-1500, March 2013.

[11] Xie, M., S. Han, B. Tian and S. Parvin, "Anomaly detection in wireless sensor networks: A survey" Journal Network Computer Application (JNCA), 1302-1325..2011.03.004, 2011.

[12] Stetsko, A., L. Folkman and V. Matyas, "Neighbor-based intrusion detection for wireless sensor networks", Proceedings of the 6th International Conference on Wireless and Mobile Communications (ICWMC), Sept. 20-25, IEEE Xplore Press, Valencia, pp: 420-425. DOI: 10.1109/ICWMC.2010.61, 2010.

[13] Lemos, M.V.D.S., L.B. Leal and R.H. Filho, "A new collaborative approach for intrusion detection system on wireless sensor networks", Novel Algorithms Techniques Telecommunication. Network DOI: 10.1007/978-90-481-3662-9_41, 2010.

[14] Supranamaya Ranjan, Ram Swaminathan, Mustafa Uysal, Antonio Nucci and Edward Knightly, "DDoS-Shield: DDoS-Resilient Scheduling to Counter Application Layer Attacks", IEEE/ACM Transactions On Networking, Vol. 17, No. 1, , pp. 26-39, February 2009.

[15] Erik Kline, Alexander Afanasyev, Peter Reiher.: "Shield: DoS Filtering Using Traffic Deflecting", 19th IEEE International Conference on Network Protocols, pp. 37-42, 2011.

[16] Ho-Seok Kang, Sung-Ryul Kim, "Design and Experiments of small DDoS Defense System using Traffic Deflecting in Autonomous System", Journal of Internet Services and Information Security (JISIS) In proceedings of MIST 2012, Vol.2, No.3, 4, pp.43-53, 2012.

[17] Intanagonwiwat, C., Govindan, R., Estrin, D., Heidemann, J. and Silva, F. (2003). Directed diffusion for wireless sensor networking, IEEE/ACM Transactions on Networking 11(1): 2-16.

[18] Vigna, G. and Kemmerer, R. A. (1999). Netstat: A network-based intrusion detection system, Journal of Computer Security 7(1): 37-71.

[19] Sun, B. (2004). Intrusion Detection in Mobile Ad Hoc Networks, PhD thesis, Texas A&M University.

[20] Chris Karlof, David Wagner, "Secure Routing in Wireless Sensor Networks: Attacks and Countermeasures", AdHoc Networks (elsevier), Page: 299-302, year 2003.

[21] Al-Sakib Khan Pathan, Hyung-Woo Lee, Choong Seon Hong, "Security in Wireless Sensor Networks: Issues and Challenges", International

Copyright © 2014 CTTS.IN, All right reserved

conference on Advanced Computing Technologies, Page1043-1045, year 2006.

[22] T.S. Sobh, "Wired and wireless intrusion detection system: Classifications, good characteristics and state-of-the-art", Elsevier J. Computer Standards and Interfaces, volume 28, number 6, pages 670-694, 2006.

[23] T. Anantvalee and J. Wu, "A survey on intrusion detection in mobile ad hoc networks", Springer J. Wireless Network Security, pages 159-180, 2007.

[24] P. Albers, O. Camp, J. Percher, B. Jouga, L. M, and R. Puttini, "Security in Ad Hoc Networks: A General Intrusion Detection Architecture Enhancing Trust Based Approaches," Proc. 1st International Workshop on Wireless Information Systems (WIS-2002), pp. 1-12, April 2002.

[25] P. Michiardi and R. Molva, "Core: A Collaborative Reputation mechanism to enforce node cooperation in Mobile Ad Hoc Networks," Communication and Multimedia Security Conference (CMS'02), September 2002.

[26] O. Kachirski and R. Guha, "Effective Intrusion Detection Using Multiple Sensors in Wireless Ad Hoc Networks," Proc. 36th Annual Hawaii International Conference on System Sciences (HICSS'03), p. 57.1, January 2003.

[27] A.P. da Silva, M. Martins, B. Rocha, A. Loureiro, L. Ruiz and H.C. Wong, "Decentralized Intrusion Detection in Wireless Sensor Networks," in Proc. 1st ACM International Workshop on Quality of Service and Security in Wireless and Mobile Networks (Q2SWinet '05), ACM Press, October 2005, pp. 16-23.

[28] P. Brutch and C. Ko, "Challenges in Intrusion Detection for Ad Hoc Networks," in Proc. IEEE Workshop on Security and Assurance in Ad hoc Networks, Orlando, FL, January 28, 2003.

[29] G. Acs and L. Buttyan, "A taxonomy of routing protocols for wireless sensor networks," Budapest University of Technology and Economics, Hungary, January 2007.

[30] J. N. Al-Karaki and A.E.Kamal, "Routing Techniques in Wireless Sensor Networks: A Survey," IEEE Wireless Communications, vol. 11, pp. 6–28, Dec, 2004.

[31] Y. an Huang and W. Lee, A cooperative intrusion detection system for ad hoc networks, in Proc of the 1st ACM Workshop on Security of Ad hoc and Sensor Networks, 2003, pp. 135–147.

[32] Y.-C. Hu, A. Perrig, and D. B. Johnson, Packet leashes: A defense against wormhole attacks in wireless networks, in Proc of IEEE Infocomm 2003.

[33] W. R. Pires, T. H. P. Figueiredo, H. C. Wong, and A. A. F. Loureiro, Malicious node detection in wireless sensor networks, in 18th Int'l Parallel and Distributed Processing Symp, 2004.

AUTHOR'S PROFILE

Phiza Ambreen Khan is presently pursuing M.Tech. in Software Technology from SSSIST, Sehore, M.P., India. Her research areas of interest include Network Security, Digital Image Processing and Fuzzy logic.

Copyright © 2014 CTTS.IN, All right reserved