ISSN: 2277-9655
Scientific Journal Impact Factor: 3.449
(ISRA), Impact Factor: 1.852

IJESRT

INTERNATIONAL JOURNAL OF ENGINEERING SCIENCES & RESEARCH TECHNOLOGY

A HIDDEN MARKOVIAN METHOD TO SECURE INTRUSION DETECTION USING RANDOM CLUSTER HEAD ALGORITHM

T.Ramesh *, S.S.Meenatchi
Assistant Professor, Department of Information Technology,
Bharathiar University, India, Coimbatore-641046
Research Scholar, Department of Information Technology,
Bharathiar University, India, Coimbatore-641046

ABSTRACT

WSN network is vulnerable to various security breaches. Depends on the application and their environment, it may vary dynamically and it is very unpredictable. In the network, each layer is prone to security breach. Designing Security measures for WSN is a challenging task. As we design more and more preventive measures for the attacks, number of attacks increases exponentially day by day. WSN has several limitations such as low energy, limited battery power, etc. So we need to consider these aspects as well while designing the system. In this paper, a new approach called Hidden Markovian Intrusion detection system is proposed which uses a new algorithm called Random Cluster Head selection. Experimental results show that the proposed model has achieved higher defense rate than any other game theoretic approaches.

KEYWORDS: Intrusion detection, WSN, Game theory

INTRODUCTION

Wireless Sensor Network (WSN) is an emerging technology which is widely used in many applications in our day to day life. Initially it was used for Military purposes and now it is being used in many commercial applications. WSN is a tiny and most sensitive device. The devices in WSN are free to move independently and it can move in any direction. There can be several paths in the networks, but WSN can choose any path that is effectively given by a router. Unlike traditional networks, it does not need any base stations. The main challenge is to maintain proper information since it switches from one network to another as often several path breaks may occur. WSN are kinds of wireless ad hoc networks.

WSN faces several constraints such as Energy, Routing, Security, Power, Memory and many more. Among these, security is a major concern. WSN in an un-attended environment is subjected to several security risks. Intruders can cause a little or huge damage that cannot be recovered.

This paper introduces the problem of Intrusions in sensor networks and takes a step towards the development and implementation of a novel approach called Hidden Markov Model (HMM) for Intrusion detection. Aiding to HMM, a new algorithm called Random Cluster Head selection (RCH) is proposed. This selects the optimal Cluster Head (CH) based on the history of node states at different instance of time.

Using attack pattern mining algorithm, time of attacks at different instance of time is recorded, based on which future attacks are predicted. The prediction time is given to the CH which in turn informs the Base Station (BS). And the base station formulates the strategy for defending the attacks.

In case of fixed CH, the nominated cluster heads are exposed to attackers which increase the chances of an attacker to devise a strategy to attack the nodes. This is a two player game, where in even the attacker can mine the pattern and attack the CH. In order to mitigate this, RCH is being proposed. By applying the RCH algorithm, the possibility of attacker to devise a strategy is made impossible, as the cluster heads are nominated on the fly. Thereby improves the overall stability of the entire network. The detailed explanation of how HMM is designed will be discussed in subsequent sections.

The remainder of this paper is organized as follows: in Section 2, we discuss Proposed Model, integrating game theory with MDP into the IDS of a WSN. In

ISSN: 2277-9655
Scientific Journal Impact Factor: 3.449
(ISRA), Impact Factor: 1.852

Section 3, we present the Simulation Result. Finally, the paper is concluded in Section 4.

All content should be written in English and should be in 2 column.

- Page type will be A4 with normal margin, word spacing should be 1.
- No space will be added before or after paragraph.
- This section should be typed in character size 10pt Times New Roman, Justified

PROPOSED MODEL

In this paper, we propose new IDS called "The Hidden Markovian IDS" where we have used game theory to select the best defense strategies and a Markovian Decision Process (MDP) to determine the weakest nodes based on the rewards assigned in the game. We have also discussed how cluster head is nominated randomly on the fly. Now, we will start discussing on the practical application of game theory with Hidden Markovian method section by section.

SYSTEM ENVIRONMENT

Assumptions:

Problems like Network congestions are not considered in this paper. And we have considered flooding attack by the intruders for our analysis.

The node deployment model considered for our discussion is as shown in Fig. 2.1. Here there two sets of sensor nodes, each containing 17 nodes reporting to a Base Station (BS). Among these two groups, any node can be nominated as Cluster head in the run time based on the Game played by the two players. For this analysis, we have considered two attacker nodes A1 & A2 which floods one of the nodes in Group1. And another attacker node A3, attacking one of the sensor nodes in Group2. Any attack to the node is reported to Cluster head which in turn is passed to Base station. So the details on how HMM and other algorithms are implemented to devise the strategy for defending the nodes under attack will be discussed going forward.

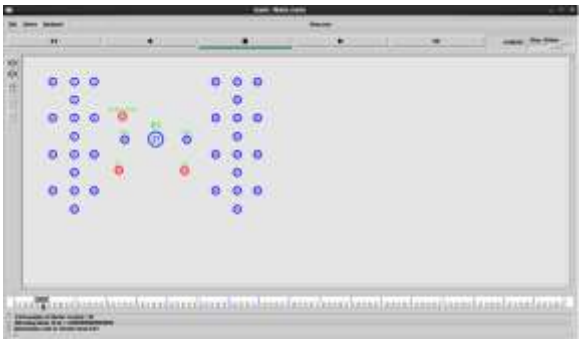

Figure 2.1 Arrangements of the nodes

PROPOSED MODEL OF HIDDEN MARKOV METHOD

In this section, the Game setup, reward function and how HMM defends and its defending strategy is defined. HMM is a statistical model, in which system is assumed to be Markov model but it has unobserved states. This is a simplest dynamic Bayesian network.

Here the attacker and the defender have their own strategies. The attacker strategies (AS) are defined as

$AS = \{as_0, as_1 \ldots asn_{-1}\}$

Similarly the defender strategy (DS) is defined as

$DS = \{ds_0, ds_1 \ldots dsn_{-1}\}$

There are 4 possible decisions for the Hidden Markov Intrusion Detection System (HMIDS). That is listed in the following table:

Table 2.1 Possible strategies

POSSIBLE STRATEGIES		HMIDS	
		MISS	DEFEND
ATTACKER	NO-ATTACK	LEAST DAMAGE	FALSE POSITIVE
	ATTACK	FALSE NEGATIVE	OPTIMAL CHOICE

If the HMIDS defends the attacks properly, then we define a reward function g as the gain. If the HMIDS does not defend the attacks, then we give the reward as –g. So that in the process of CH selection, if it has the reward value as –g then it will not be selected as CH.

When the process state "s" in a time interval t can be defined as "st", then the defender strategy can be taken based on the rewards assigned to the nodes at any instance of time.

At any instance of time, we define function (f) for defense (ds) and attacking strategy (as).

$$f: \rightarrow ds\ X\ as$$

Using this we calculate the reward function, r for the states at each instance of time.

ISSN: 2277-9655
Scientific Journal Impact Factor: 3.449
(ISRA), Impact Factor: 1.852

$$r(f(s_t)) = \begin{cases} 0 & if\ i = 0, j = 0 \\ \delta_i(g - c_i) & if\ i \neq 0, j = 0 \\ -g & if\ i = 0, j \neq 0 \\ g_{k_{ij}} - c_i & if\ i \neq 0, j \neq 0 \end{cases} \text{---------- (1)}$$

This is the reward function for all the 4 possible strategies. And the last strategy is the best one as it defends most of the attacks. Here, i is the attacker variable and j is the defender variable.

We assume that the state of node x is s0 at t = 0. If defense strategy d is taken against attack strategy a, the state of node x evolves from s_0 to s_1, and node x receives a reward r(f(s_0)) and so on, as shown by Eq. (2). In the Hidden Markovian Decision Process (HMDP), the state of node x transits from s_0 to s_1 and eventually to sp, where $1 \leq p \geq k - 1$. Thus, the accumulated reward received by x is as follows:

$$r_x^p = r(f(s_0)) + \gamma r(f(s_1)) + \gamma^2 r(f(s_2)) + \cdots + \gamma^p r(f(s_p)) \text{---------- (2)}$$

Where$\gamma \varepsilon (0,1)$ is the discount rate parameter.

At a discount rate of 0, the system considers only the current reward, but at a value of 1, it would regard the long-term high reward. The objective of the HMIDS is to choose an appropriate defense strategy against an attack strategy to accumulate rewards

$$r_x^p = \Sigma_{t=0}^{p} \gamma^p r(f(s_p)) \text{ ---------- (3)}$$

Table 2.2 Definitions of the notations in Attack Pattern mining

T	Time durations
S	State space of a node
Ds	Defense strategies
As	Attacker strategies
G	Reward
k_{ij} ε[0,1]	Effectiveness of the reward
δ_i ε[0,1]	False positiveness of the reward
c_i	Denotes the cost

A. PROPOSED ALGORITHM

In this paper, 2 algorithms are used and the detailed information of both are given below:

i. *ATTACK PATTERN MINING*

This algorithm is used to record the pattern of time of attacks at different instances. This information is being sent to the CH, which in turn forwards the information to the BS. The purpose of this algorithm is to record the pattern of attacks and based on the recorded data, the future attack is predicted. The advantage of implementing this frame work improves the chance of detecting intrusion in an optimal way. In this framework, we have different types of nodes they are

I. Sensor nodes
II. CH
III. BS

I. SENSOR NODES

Sensor nodes are members of a cluster. These nodes sense the data and they can share their information to other sensor nodes. They have designated CH which is also a normal sensor node. Any information to the Base station is communicated via CH. It has no direct connection with the Base Station.

II. CLUSTER HEAD

Each node in the network is connected with one CH. CH is connected with the Base Station. The CHs and the BS forms a backbone. This connected backbone helps in detection of Intruder and appropriate defense mechanism is taken.

III. BASE STATION

This is the root node, it controls all other nodes. This takes appropriate decision and instructs the CH to execute. If the decision taken by the BS is not an appropriate defensive strategy, BS revises the decision and instructs back to CH. It uses Bayesian approach for taking the decision.

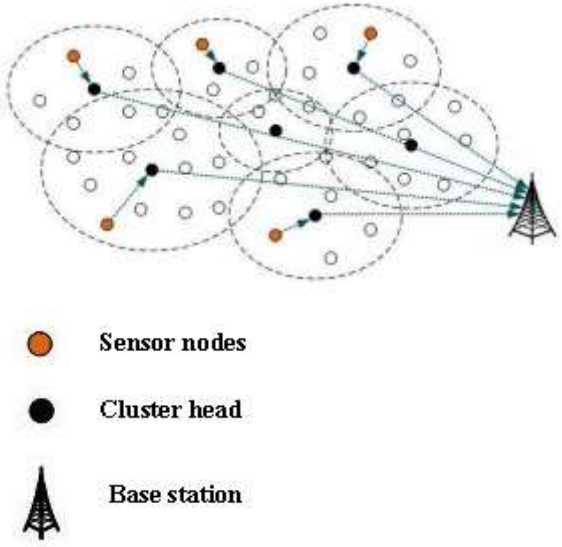

Figure 2.1 Attack pattern mining

In our system, HMIDS records the pattern of attacks using pattern mining algorithm and predicts the next time of attack. We have provided additional buffer time of 0.5 sec and starts defending the nodes before

ISSN: 2277-9655
Scientific Journal Impact Factor: 3.449
(ISRA), Impact Factor: 1.852

the predicted time of attack. The notations used in the algorithm are:

Table 2.3 Notations used in Attack Pattern Mining

Notation	Explanation
Tba	Time Between Attack
AvgTba	Average of time between attack
AP	Attack Pattern
Toa	Time of attack
Ptoa	Predicted time of attack
N	Number of attacks

A. DESIGN OF THE ALGORITHM

Step 1: Record the time of attacks at regular intervals as

$\sigma = (toa_1, toa_2 ... toa_m)$ ---------- (4)

Where σ denotes the sequences toa is the time of attack that are recorded in the regular time intervals.

Step 2: Calculate the Time between Attacks

$\delta = (toa_{n-1} - toa_n)$ ---------- (5)

Where δ denotes Time Between the attack toa denotes the time of attack.

n represents the number of attack

Step 3: From the previous step, the attack intervals are stored in the system. Now we can calculate the average time as

$avgTba = \frac{(\Sigma(toa_1)+\cdots+(toa_{n-1})+(toa_n))}{n}$ ---------- (6)

Where, avgTba is the average time between attacks.

toa denotes the time of attack

n represents the number of attack

Step 4: From the average calculated, we predict the future attack.

$pToa = (toa_c + avgTba) - buf$ ---------- (7)

Where pToa is the Predicted time of attack, Toa_c denotes the current time of attack, buf denotes the buffer time in seconds. avgTba denotes the average time between attack

Step 5: Based on the possibilities defined in table 3.1, appropriate security measure is taken by the defender.

The above steps are described below:

Process begins whenever there is an attack in the cluster. Whenever there is an attack, then the time of attack is being recorded in the base station, so that we can calculate the parameters like time between attack and avgTba. Based on which the future attack is predicted.

To calculate the time between attacks the formula used is given below

$\delta = (toa_{n-1} - toa_n)$

Here the time between attacks is stored in the base station. We take that in account and calculate the time between attacks.

For example if the time of the first attack has occurred in 5th minute and the next attack has occurred in 10th minute, the time between attacks is 10-5 = 5 minutes.

Next is to calculate average time between attacks. This is calculated as

$avgTba = \frac{(\Sigma(toa_1)+\cdots+(toa_{n-1})+(toa_n))}{n}$

Using this average, we have to predict the future attack using

$pToa = (toa_c + avgTba) - buf$

Here we need to provide some buffer in seconds so that even before we expect an attack the system starts defending for more stability. As per our previous example the time of attacks happens at 5th and 10th minute, so that the next predicted attack will be at 15th minute. After the prediction using mining algorithm the next step is to devise an appropriate strategy to defend the attacked nodes. For that the states of the different nodes are considered. Like discussed earlier reward points are calculated based on the game results between the two players.

ii. RANDOM CLUSTER HEAD SELECTION ALGORITHM

Static CH exposes the state of nodes to the intruder. So in order to hide the state and identity of the nodes to the intruder, a new algorithm called RCH is proposed. This algorithm nominates the CH based on the history and state of the nodes randomly. New CH is selected based on how well that particular node is performing. The following figure illustrates the Random CH selection.

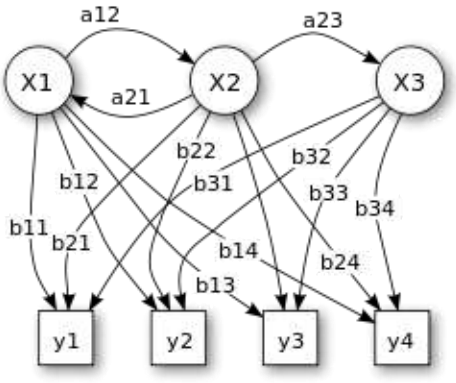

Figure 3.2 Random CH Selections

ISSN: 2277-9655
Scientific Journal Impact Factor: 3.449
(ISRA), Impact Factor: 1.852

Here x defines the possible states, y defines the possible observations, a defines the state transition probabilities and b defines output probabilities. The random variable x(t) is the hidden state at time t (x(t) €{ x1, x2, x3 }). The random variable y(t) is the observation at time t (with y(t) €{ y1, y2, y3, y4 }). The arrows in the diagram denote the conditional dependencies.

A) DESIGN OF THE ALGORITHM

Step 1: Identify the physical cluster.
Step 2: Input the data's
Step 3: Split the nodes individually.
Step 4: Calculate the reward values for all the nodes at different instances to select the CH.
This is given as

$$r_x^p = r\big(f(s_0)\big) + \gamma r\big(f(s_1)\big) + \gamma^2 r\big(f(s_2)\big) + \cdots + \gamma^p r\left(f(s_p)\right)$$

Here r_x^p denotes the reward function for the predicted attack at a period of time
f denotes the function
s denotes the state of transmission
γ denotes the discount rate parameter
Step 5: Check the reward function.
Step 6: If the reward function is less than 5 then do not nominate the node for CH selection.
Step 7: If the reward function is greater than 5 nominate them for CH selection
Step 8: The CH nominated and rejected nodes are stored in the database.
Step 9: Based on the stored values the nominated CH is compared and the highest rewarded node is selected. If it contains more than one same reward value it selects randomly.
The above steps are described below:

Based on the input data's we begin our process. We split all our nodes to calculate the reward value. The reward value is calculated by using the following formula

$$r_x^p = r\big(f(s_0)\big) + \gamma r\big(f(s_1)\big) + \gamma^2 r\big(f(s_2)\big) + \cdots + \gamma^p r\left(f(s_p)\right)$$

This reward value is the most important for the random cluster head selection. By default each node is assigned the reward value as 5. If any attack occurs the counter is reduced by 1 and if it defends properly we increment the counter by 1.

After calculating the reward value based on the attacks, the CH selection begins. Here we have a comparison between nodes if it is greater than 5 it is nominated for CH selection or if it is less than 5 the node is not sent for CH selection.

This information is stored in the database. The node which has the greater reward value is selected as CH. If more than one node contains the same reward value for each instances of time the nodes are selected randomly.

SIMULATION RESULT

The results from the simulation have shown below in the table and the related line graph with variable time. In the table 3.1 the time vs. packet drop ratio compared to existing work is recorded and portrayed in the subsequent figures. The defending strategy is done for flooding attack. In the table 3.2 a comparison chart between existing and proposed Time vs. Packet Delivery Ratio.

Table 3.1 Time Vs. Packet drop

Time	Existing (Fixed CH)	Proposed (Random CH)
1.9	4	4
4	7	6
6	8	2
8	4	0
10	3	0
12	3	0
14	1	0
16	2	0
18	3	0
20	4	0

Table 3.2 Time Vs. Packet delivery Ratio

Time	Existing (Fixed CH)	Proposed (Random CH)
0	0.80	0.80

ISSN: 2277-9655
Scientific Journal Impact Factor: 3.449
(ISRA), Impact Factor: 1.852

2	0.45	0.50
4	0.40	0.40
6	0.70	0.72
8	0.35	0.75
10	0.30	0.80
12	0.25	0.82
14	0.32	0.85
16	0.31	0.90
18	0.33	0.85
20	0.40	0.80

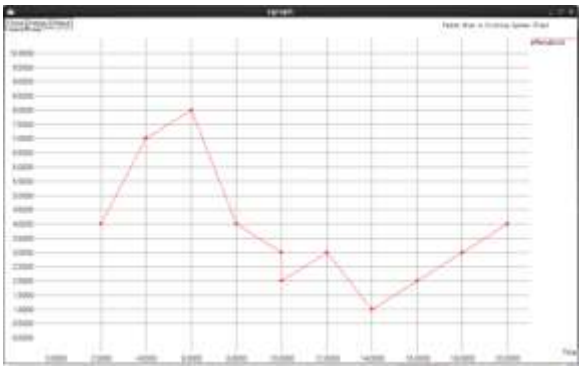

Figure 3.1 Packet drop in the existing system

The above figure shows the packet drop induced in the existing system due to the highlighted flaw (State of the node is visible) in this thesis. From the graph we understand that few attacks had happened at 2.0, 4.0 & 6.0 seconds respectively. Ideally after sixth second, intrusion detection system should predict the attack pattern and defend the node under attack accordingly. But in this case, since CH itself is attacked by the attacker, the prediction of the future attack is prevented resulting in failure in defending the node under attack. From the above observation, even after the second attack, the packets are getting dropped due the failure in communication to base station from cluster head. This situation will finally lead to a network congestion which would break the system.

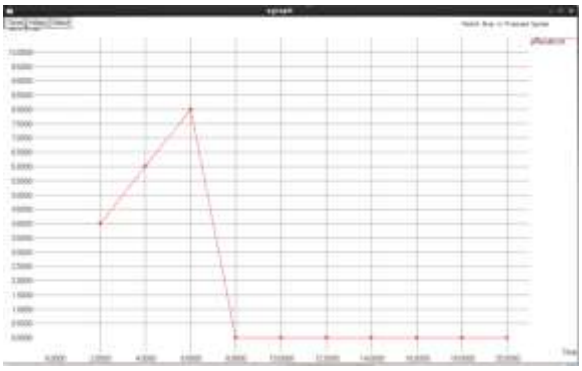

Figure 3.2 Packet drop in the proposed system

The above figure highlights the benefits we have yielded after implementing the hidden markovian model to our system. Here as we notice, once HMM enabled security system comes into picture, the packet drop gets drastically reduced to zero. From then on, all the nodes are successfully defended and health of the entire network is maintained. There is not even a single packet drop which is a clear indication of the successful defensive strategies devised by the defender as a player.

The below figure finally compares both the output in a single graph thereby highlighting the benefits gained in proposed system.

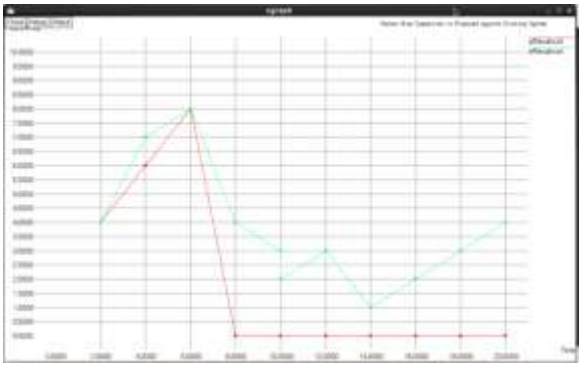

Figure 3.3 Packet drop comparison in existing system Vs. Proposed system

ISSN: 2277-9655
Scientific Journal Impact Factor: 3.449
(ISRA), Impact Factor: 1.852

Figure 3.4 Packet Delivery Ratio in Proposed system

The above figure shows the Packet Delivery Ratio in the Proposed System. As our Hidden Markov Approach defends in a good way the packet delivery ratio increases. In the Existing system if the CH is defeated then attack increases so that the Packet Delivery Ratio in the Existing System Decreases.

In the below figure, Packet Delivery Ratio between Existing and Proposed System is being compared.

Figure 3.5 Packet Delivery Ratio in existing system Vs. Proposed system

CONCLUSION

Testing and experimenting was the hardest part of this work. Even though Ns2 provides useful features to debug an application, it is sometimes not easy to find the cause of a problem in a distributed application. Securing every node is the most important criteria. In this thesis two securing algorithms provides better results than the existing. Improved Intrusion detection mechanism using HMM a game theoretic approach is given. This part of the work gave us a good experience about experimentation techniques and problems for securing WSN.

In Intrusion detection system, the cluster head selection is the most important part which will improve the quality of tracking the data. The proposed Random Cluster Head selection (RCH) algorithm is implemented to select the best cluster heads to monitor the nodes in order to keep track the node and also to defend the attackers. Thus an enhanced version of intrusion detection using Hidden Markovian Approach is proposed.

This approach overcomes the problem in the existing markovian approach wherein if a CH is attacked, then the entire effort taken while defending becomes vain. In this approach a CH is not revealed to the attacker. As the CH is not static even if the attacker attacks the correct CH that is pattern mined and another CH is nominated which communicates the attack to Base station and defends the attack. Experimental results verify that the proposed algorithm can enhance the Intrusion detection and defend the intruders using Hidden Markov Method.

REFERENCES

[1] Anitha S Sastry, ShaziaSulthana, Dr. S Vagdevi , " Security Threats in Wireless Sensor Networks in Each Layer " , Int. J. Advanced Networking and Applications Volume: 04 Issue: 04 Pages:1657-1661 (2013) ISSN : 0975-0290

[2] Afrand Agah1 and Sajal K. Das2, "Preventing DoS Attacks in Wireless Sensor Networks: A Repeated Game Theory Approach". In: International Journal of Network Security, Vol.5, No.2, PP.145–153, Sept. 2007

[3] Asim Kumar Pal, DebabrataNath and SumitChakraborty, "A Discriminatory Rewarding Mechanism for Sybil Detection with Applications to Tor" in:World Academy of Science, Engineering and Technology 39 2010

[4] Feng, W., Kaiser, E., Luu, "A.: Design and implementation of network puzzles." In: INFOCOM 2005. 24th Annual Joint Conference of the IEEE Computer and Communications Societies. Proceedings IEEE, March 2005, vol. 4, pp. 2372–2382(2005)

[5] Hai-Yan Shi, Wan-Liang Wang ,Ngai-Ming Kwok and Sheng-Yong Chen, "Game Theory for Wireless Sensor Networks: A Survey

ISSN: 2277-9655
Scientific Journal Impact Factor: 3.449
(ISRA), Impact Factor: 1.852

"Sensors 2012, 12, 9055-9097; doi:10.3390/s120709055

[6] Harikrishna Narasimhan1, VenkatanathvdcanVaradarajan and C. PanduRangan "Game Theoretic Resistance to Denial of Service Attacks Using Hidden Difficulty Puzzles"In: J. Kwak et al. (Eds.): ISPEC 2010, LNCS 6047, pp. 359–376, 2010.Springer-Verlag Berlin Heidelberg 2010

[7] HandeAlemdar, CemErsoy, "Wireless sensor networks for healthcare: A survey", Elseiver , Computer Networks 54 (2010) 2688–2710

[8] Hongjun Dai, Yu Liu, FenghuaGuo and ZhipingJia, "A Malicious Node Detection Algorithm Based on Principle of Maximum Entropy in WSNs", JOURNAL OF NETWORKS, VOL. 7, NO. 9, SEPTEMBER 2012.

[9] Hoang Nguyen, ThadpongPongthawornkamol and KlaraNahrstedt, "Alibi: A framework for identifying insider-based jamming attacks in multi-channel wireless networks" Published in: Proceeding MILCOM'09 Proceedings of the 28th IEEE conference on Military communications Pages 2646-2652 IEEE Press Piscataway, NJ, USA ©2009 ISBN: 978-1-4244-5238-5

[10] Idris M. Atakli, Hongbing Hu, Yu Chen, Wei-Shinn Ku , Zhou Su "Malicious Node Detection in Wireless Sensor Networks using Weighted Trust Evaluation " The Symposium on Simulation of Systems Security (SSSS'08), Ottawa, Canada, April 14 – 17,2008.

[11] Jen-Yan Huang , I-En Liao Yu-Fang Chung , Kuen-Tzung Chen, "Shielding wireless sensor network using Markovian intrusion detection system with attack pattern mining" Elsevier, Information Sciences 231 (2013) 32–44

[12] KanthakumarPongaliur · Li Xiao · Alex X. Liu, "Dynamic camouflage event based malicious node detection architecture",Springer Science+Business Media, LLC 2010, J Supercomput (2013) 64:717–743 DOI 10.1007/s11227-010-0508-x.

[13] Luis Ruiz-Garcia,LoredanaLunadei, Pilar Barreiro and Jose IgnacioRobla "A Review of Wireless Sensor Technologies and Applications in Agriculture and Food Industry: State of the Art and Current Trends ", Sensors 2009, 9, 4728-4750; doi:10.3390/s90604728.

[14] Luís M. L. Oliveira, Joel J. P. C. Rodrigues, "Wireless Sensor Networks: a Survey on Environmental Monitoring ", JOURNAL OF COMMUNICATIONS, VOL. 6, NO. 2, APRIL 2011.

[15] LEKSHMI.M.R, N. NITYANANDAM, "Thwarting Selective Insider Jamming Attacks in Wireless Network by Delaying Real Time Packet Classification" Indian Journal of Computer Science and Engineering (IJCSE)Vol. 4 No.3 Jun-Jul 2013

[16] Manfred J. Holler, "Classical, Modern and New Game Theory ", Institute of Socio Economics, University of Hamburg, Von-Melle-Park 5, D-20146 Hamburg, Germany.

[17] Mehran S. Fallah "A Puzzle-Based Defense Strategy against Flooding Attacks Using Game Theory". InIEEE TRANSACTIONS ON DEPENDABLE AND SECURE COMPUTING, VOL. 7, NO. 1, JANUARY-MARCH 2010.

[18] Michal VARCHOLA, Miloš DRUTAROVSKÝ, "ZIGBEE BASED HOME AUTOMATION WIRELESS SENSOR NETWORK", ActaElectrotechnicaetInformatica No. 4, Vol. 7, 2007

[19] Renita Machado, SirinTekinay , "A survey of game-theoretic approaches in wireless sensor networks" , Elseiver, Computer Networks 52 (2008) 3047–3061.

[20] Seo Hyun Oh, Chan O. Hong, Yoon-Hwa Choi,"A Malicious and Malfunctioning Node Detection Scheme for Wireless Sensor Networks",Scientific research, Wireless Sensor Network, 2012, 4, 84-90 doi:10.4236/wsn.2012.43012 Published Online March 2012.

[21] Sung Yul Lim and Yoon-Hwa Choi, "Malicious Node Detection Using a Dual Threshold in Wireless Sensor Networks",Journal of Sensor and Actuator

ISSN: 2277-9655
Scientific Journal Impact Factor: 3.449
(ISRA), Impact Factor: 1.852

Networks, J. Sens. Actuator Netw. 2013, 2, 70-84; doi:10.3390/jsan2010070.

[22] SudipMisra , Sanjay K. Dhurandher , AvanishRayankula , DeepanshAgrawal , "Using honey nodes for defense against jamming attacks in wireless infrastructure-based networks", Elsevier, Computers& Electrical Engineering, pg. 367-382,Vol. 36, Issue 2, March 2010.

[23] T. Alpcan and T. Basar, "A Game theoretic analysis of intrusion detection in access control systems," in Proc. of the 43rd IEEEConference on Decision and Control, Paradise Island, Bahamas, December 2004, pp. 1568–1573.

[24] Teresa M.A. Basile, Nicola Di Mauro, Stefano Ferilli, and Floriana Esposito, "Relational Temporal Data Mining for Wireless Sensor Networks"

[25] WenjingWang, MainakChatterjee and Kevin Kwiat, "Coexistence with Malicious Nodes: A Game Theoretic Approach" In: July 21, 2009 IEEE Xplore.

[26] Yenumula B Reddy, S. Srivathsan. "Game Theory Model for Selective Forward Attacks in Wireless Sensor Networks"In: 17th Mediterranean Conference on Control &AutomationMakedonia Palace, Thessaloniki, Greece June 24 - 26, 2009.

[27] Yu Liu, Cristina Comaniciu,Hong Man "A Bayesian Game Approach for Intrusion Detection in Wireless Ad Hoc Networks" In: 2006 ACM 1-59593-507-X.

Author Biblography

T.Ramesh
Received the Master's Degree in Computer Application from Anna University, Tamil Nadu, India in 1996, M.Phil, degree in Computer Science from Bharathiar University, Coimbatore, Tamil Nadu, and India in 2008 and M.Tech(IT) from Anna University, Coimbatore. He is currently working as Assistant Professor and Assistant Technical officer in Department of Information Technology, School of Computer Science and Engineering, Bharathiar University, India, Coimbatore-641046. He is having more than 18 years of experience as teaching and research. He has published 20 articles in National, International Journals and International Conference and written Two books. His current research includes: Computer Networks, Mobile Computing, and Information Security.

S.S.Meenatchi
Received her Master's Degree in Computer Science and Information Technology from G.T.N Arts College, Dindigul, Tamil Nadu, India in 2007.Worked as Lecturer for1 year in G.T.N Arts College, Dindigul, Tamil Nadu, India. Completed M.Phil (Research Scholars), in Computer Science , School of Computer Science and Information Technology, Bharathiar University , India, Coimbatore -641046.
Has attended 1 National conference and published 3 articles in National Journals.
Her area of interest includes: Network Security, WSN, Game theory.