DEFENSIVE MEASURES FOR TOPOLOGY MAINTENANCE PROTOCOLS

Barigala Lydia Sravanthi[1], Yaramati Sarada Devi[2],
Pulabam Soujanya[3], T. Dharma Reddy[4]

[1]Department of CSE, CMR College of Engg. and Technology, Hyderbad, A. P., India.

[2&3]Assistant Professor & [4]Professor,
Department of CSE, CMR College of Engg. and Technology, Hyderbad, A. P., India

ABSTRACT

In this paper, the security vulnerabilities of topology maintenance protocols namely PEAS, CCP which are used in sensor networks are analyzed. Each node in the network will be in either Sleep or Active State. In Active State, a node performs sensing coverage functionality, in sleep state a node will sleep for a random period of time. These protocols require message exchange between a node and its neighboring nodes, to enable the node to be in active or sleep state depending on the information it received in the message from its neighboring nodes. Thus these protocols are vulnerable to security attacks in which malicious nodes send spoofed or false messages between nodes to make a node remain in Active or in Sleep State for a longer time i.e. in non-selected periods of time which degrades the functionality of sensor application. If a node remains in active state or sleep state for a longer time i.e. in non-selected periods of time, either energy expenditure of the sensor node is increased or connectivity of network and sensing coverage in a particular area is affected. Subsets of active nodes are to be maintained by the protocols to ensure network connectivity and sensing coverage for sensor networks (sensor applications). Three attacks against these protocols carried by an adversary to reduce the lifetime of the sensor network, and counter measures that make sensor network resilient to these attacks are described in this paper.

KEYWORDS: *Wireless Sensor Network, Energy Conserving Robust Network Protocol, Authentication, Data Integrity, Security.*

I. INTRODUCTION

For the operation of wireless sensor networks, topology maintenance protocols are important. These protocols turnoff redundant nodes, maintain a subset of active nodes for the functionality of sensor application. To maintain connectivity of the network and to obtain sensing coverage in the sensor network deployment area, sufficient active nodes are required. Every node in the network decides to be in active or sleep state depending on the messages it received from its neighbor nodes .An adversary sends false messages, to make nodes remain in active or sleep state for longer time in non-selected periods in order to degrade the functionality of sensor network. Three types of attacks are carried out by an adversary by inducing spoofed messages, namely sleep deprivation attack ,snooze attack, network substitution attack. Sleep Deprivation attack aim is to make a node remain in working state for a longer time which yields to increased energy expenditure of sensor nodes, and thus reduces the lifetime of the sensor network; Snooze attack aim is to make a node remain in sleep state for a longer time, which results in inadequate sensing coverage or network connectivity; In Network Substitution attack ,adversary takes control of portion of sensor network by using set of malicious

nodes. To prevent these attacks countermeasures are proposed which includes authentication mechanisms i.e .messages exchanged between nodes have to be authenticated.
The rest of this paper is organized as follows: in Section 2.Related work is described, in Section 3.Review of protocols is presented, in Section 4.Attacks, in Section 5. Counter Measures, in Section 6. Results & Discussions, in Section 7.Conclusion & Future Work are described.

II. RELATED WORK

In this section topology maintenance protocols and attacks against these protocols are described. PEAS a robust energy-conserving protocol that can build long-lived resilient sensor networks using a very large number of small sensors with short battery lifetime.CCP maintains sensing coverage area of the network by keeping the number of active sensor nodes small to achieve long system life time .Both protocols maintain functionality of the network by keeping only a necessary set of sensors in working mode and the rest of nodes in sleep mode. Sensor nodes in the network do not maintain any information of their neighbors and topology .When a node wakes up, it needs to decide whether it should be in the working or sleep mode depending on the messages it has received from its neighbor node. The wake up frequency of sleeping node is self-adjusted to maintain both working node density and to minimize energy consumption .If an adversary compromises a node ,all information related to cryptographic keys are captured. Therefore the attacker clones the identity of compromised node and sends false messages to neighbors to make them remain in active or sleep state for a longer time. If a node remains in active state for a longer time in non-selected periods, energy expenditure of the sensor node is increased. If a node remains in sleep state for a longer time it affects connectivity of network and also reduces sensing coverage in a particular area. A node includes its Identity, Position and State of activity in its message and sends to its neighbor nodes, depending on which receiving node decides to be in active or sleep state .An adversary clones the identity of compromised nodes by sending false message to their neighbors which includes incorrect ID or position or state of activity, thereby making the node to be in active or sleep state for longer time, thus results in degraded functionality of sensor application. In Sleep deprivation attack adversary makes a node to be in working state until all its energy is consumed. In Snooze attack, adversary makes a node to be in sleep state for a longer time. In Network substitution attack adversary deploys set of nodes that are included in the set that has been elected by topology maintenance protocol to maintain network connectivity, thereby takes portion of the network under its control. All these three attacks are carried out by sending false messages to neighbors. Therefore the objectives of the topology maintenance protocol will not be achieved, thus leading to degraded functionality.

III. BRIEF REVIEW OF PROTOCOLS

3.1 BRIEF REVIEW OF PEAS

PEAS operations can be classified into two sections namely: Probing Section and Sleeping Section.

3.1.1 Probing Section

Each node in the PEAS has three operational modes: Sleeping .Probing and Working. Initially few nodes will be in the Sleeping mode. Each node sleeps for an exponentially distributed duration generated by a Probability density function(PDF) ,$f(T_s)=\lambda e^{-\lambda T_s}$, where λ is the probing rate of the node, which is adjusted according to the sleeping algorithm, this takes information carried in REPLY message as input and T_s denotes the length of sleeping time. PROBE and REPLY are the messages exchanged between nodes. A node in Sleeping mode waits until its sleeping time expires, and then, enters the Probing mode. In the Probing mode, a sensor tries to detect whether any working node is present within a probing range R_p. The probing node sends a PROBE message within a range of R_p, and any working node within R_p should respond with a REPLY message, which is also sent within the range of R_p. If the probing node receives a REPLY with the working time greater than its working time, it goes back to Sleeping mode, else if it receives REPLY with the working time lesser than its working time or no reply from its neighbors, it remains in working mode. When a node probes multiple working nodes may exist within range R_p. To reduce collisions, each working node waits for a small random period before it sends the reply .If the node does not hear any REPLY it stays in the

Working mode until all its energy is consumed. The Probing range R_p determines the redundancy of working nodes.

3.1.2 Sleeping Section

PEAS allows to adjust probing rate of sleeping nodes .Each working node measures the aggregate probing rate $\hat{\lambda}$ from all its sleeping neighbors.

3.1.2.1 Aggregate probing rate measurement

Each working node maintains two variables N and t_o ,where N is a counter that is incremented by 1 each time a PROBE is received and t_o is time when N is set to 0(i.e. initial time).When the counter reaches threshold value ,aggregate probing rate is calculated by using the below formula,

$\hat{\lambda} = k/(t - t_o)$

where k is the threshold value i.e. maximum value(i.e. k=32) up to which N can be incremented and 't' is the current time. The working node then includes the measured aggregate probing rate $\hat{\lambda}$ and desired probing rate λ_d in its REPLY in response to the PROBE.

3.1.2.2 Updation of probing rate

Upon receiving a REPLY message from the working node, the probing node updates its current probing rate λ^{new} based on the received aggregate probing rate $\hat{\lambda}$ i.e.

$\lambda^{new} = \lambda \ (\lambda_d/\hat{\lambda})$,where $\hat{\lambda}$ is the aggregate probing rate, λ_d is the desired probing rate ,λ is the old probing rate.

$f(T_s) = \lambda^{new} e^{-\lambda new (Ts)}$,where $f(T_s)$ is the new sleeping period generated according to the probability density function.

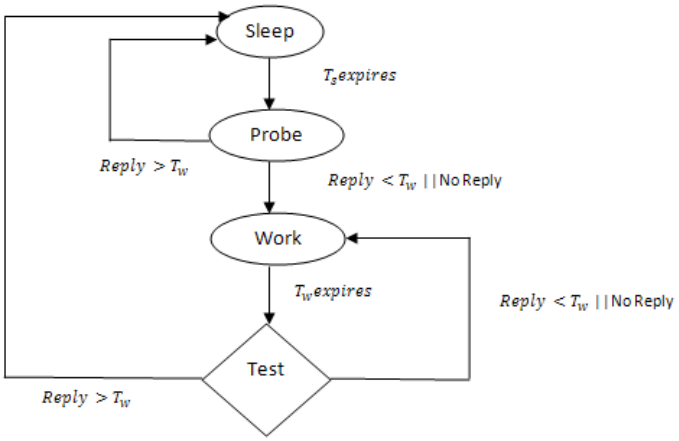

Figure 1: Working Of PEAS

3.2 BRIEF REVIEW OF CCP

Each node in the CCP can be in one of the three states: Sleep, Listen, Active. In Sleep state, a node sleeps until its sleep timer T_s expires. Then it wakes up, it starts a listen timer T_L and enters the LISTEN state. Here are some definitions required to be understood before going into Listen state. The sensing circle of a node 'A' is the set of nodes that are at some distant 'x' from node 'A'. An intersection point is the intersection between two sensing circles, or is the intersection between the sensing circle of a node and the boundary of the area to be covered. The coverage eligibility rule is that a node 'A' is not eligible to become active if there is a node 'B' that is an intersection point between the sensing circles of two active nodes and is also within the sensing circle of node 'A' .In the LISTEN state, the node collects beacon messages, i.e., locally broadcast HELLO, WITHDRAW, and JOIN messages, and executes the coverage eligibility rule. Each node decides to be in active or sleep state by using the coverage eligibility rule and the information that is received in the beacon messages sent by its neighboring nodes. If the node is eligible, it enters the ACTIVE state and

broadcasts a JOIN message; otherwise, when T_L expires, it starts a sleep timer T_s and goes back to the SLEEP state. In Active state, node remains till T_w expires, then starts receiving beacon message's, and executes the coverage eligibility rule to determine its eligibility. If it is noneligible, it sends a WITHDRAW message and goes back to sleep, else remains in Active State.

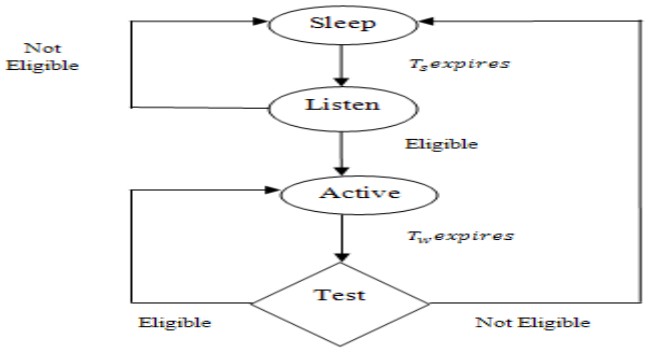

Figure 2: Working of CCP

IV. ATTACKS ON BOTH PEAS & CCP

4.1 SNOOZE ATTACK

The goal of this attack is to keep all nodes in sleep state for a longer time in non-selected periods . An adversary within the probing range of a working node sends a forged REPLY. In the forged REPLY, T_w is set to the maximum value it can have. Each working node goes to sleep because it believes that there is another working node within its probing range and with a greater T_w(Working Time). Further, the adversary can use the $\hat{\lambda}$ value included in the REPLY message to control the sleep schedules of other nodes. For instance, it can set a small $\hat{\lambda}$ to make other nodes wake up very often and rapidly consume their energy. In order to disable the network during selected periods of time, the adversary can use a large value for $\hat{\lambda}$, and thus, make other nodes to sleep for a long time.

4.2 SLEEP DEPRIVATION ATTACK

The goal of this type of attack is to keep all nodes in working mode for a longer time in non-selected periods. The adversary puts all the nodes in sleeping mode by sending false message. When all the nodes wake up to probe, the attacker jams the network to prevent any of them from receiving a REPLY. Since none of them received REPLY, all the nodes go to Working mode. Thus an adversary makes all nodes to stay in working mode even in non selected period of time leading to increased energy expenditure of sensor node.

4.3 NETWORK SUBSTITUTION ATTACK

In this type of attack, the adversary takes control of the entire network or a portion of it by deploying set of malicious nodes in the set that has been elected by the topology maintenance protocol to maintain network connectivity or the sensing of the area.

V. COUNTER MEASURES

Proposed counter measures ensure authenticated communication between nodes. Messages exchanged between nodes in the TMPs are local broadcast messages, i.e., each node broadcasts messages to its immediate neighbor nodes .The aim of using authenticated communication between nodes is to detect false messages injected by an adversary. Proposed measure for PEAS include pairwise key establishment with neighbor nodes ,sending message along with message authenticated code generated using shared pairwise key .Proposed measure for CCP include pairwise key establishment with neighbor nodes ,sending message along with a key generated from LEAP's One Way key chain mechanism for authentication purpose. Establishment of shared pairwise key is common for both (PEAS, CCP) proposed measure. Steps to establish shared pairwise keys is as below:

5.1 SHARED PAIRWISE KEYS ALGORITHM

Step1: Controller generates an initial key KI and loads each node with this key.

Step2: Node generates Master key from initial key i.e. node 'x' derives Kx=fKI(x) from KI.

Step3: Node broadcasts HELLO message which contains its ID i.e. node 'x' sends x→ *: x to all neighbors.

Step4: Node receives reply in response to HELLO from its neighbor, which contains neighbor ID and MAC i.e. y→x:y,MAC(Ky,x | y) ;MAC is generated by neighbor using its Master key.

Step5:Node generates master key of neighbor , using ID of neighbor and initial key i.e. Ky=fKI(y),where 'y' is neighbor of 'x'.

Step6:Node 'x' computes MAC by taking ID 'y' and Master key 'Ky' of neighbor.

Step7:Node verifies reply, by comparing its(node's) MAC and neighbor nodes MAC. If both MAC's are same goes to step 7,else discards the reply.

Step8:Node 'x' computes pairwise key with neighbor 'y' i.e. Kxy=fKy(x); Kxy serves as the shared pairwise key between node x and node y.

Step9**:** Node erases all master keys of its neighbors, computed in step5 ,after expiration of its time.

5.2 PROPOSED ALGORITHM FOR PEAS

Step1:Establish pairwise keys with neighbors using the above Shared Pairwise Keys algorithm.

Step2: After expiration of sleeping time, node sends PROBE containing nonce and ID to all its neighbors i.e. node 'x' sends x→* : PROBE, x,nonce;

Step3:Node receives REPLY sent by its neighbor which includes MAC computed with the shared pairwise key Kxy. i.e. node 'x' receives y →x: REPLY, y, $\lambda^{\wedge}$,Tw, MAC(Kxy;REPLY | nonce |$\lambda^{\wedge}$ |Tw);where 'y' is ID, $\lambda^{\wedge}$ is the Probing Frequency and Tw is the Working time.

Step4:Node 'x' computes MAC by taking REPLY as input and shared pairwise key using MAC algorithm.

Step5: REPLY is authenticated by node 'x' ,by comparing its MAC with neighbor nodes MAC.

Step6:If both MAC's are same , node 'x' takes information from REPLY sent by its neighbor and decides to go to working or sleep state ,else discards REPLY.

Note: If LEAP is used to establish the pairwise keys, the adversary cannot reuse the compromised nodes at different locations in the network.

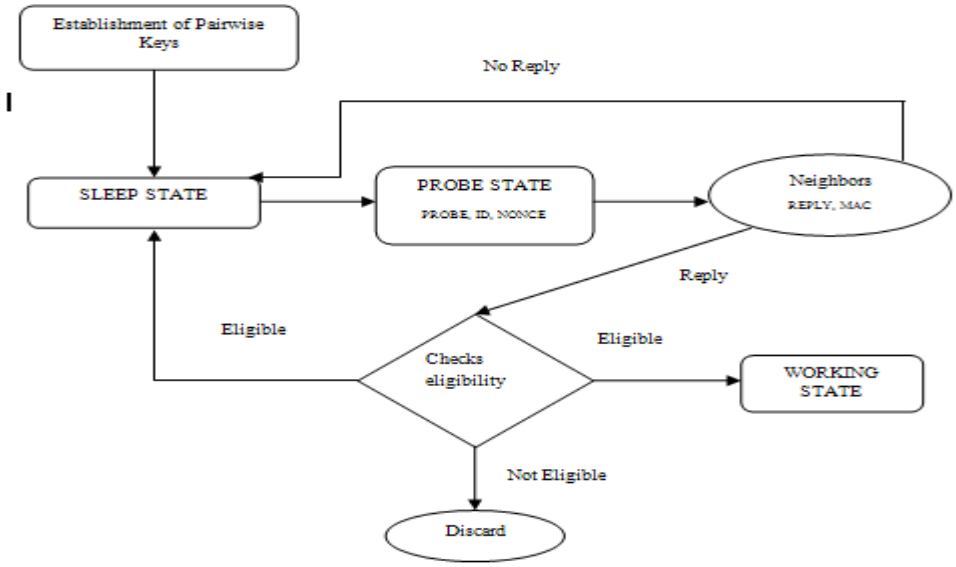

Figure 3: Defensive Measure for PEAS

5.3 PROPOSED ALGORITHM FOR CCP

Step1: Establish pairwise keys with neighbors using the above Shared Pairwise Keys algorithm.

Step2: After expiration of sleeping time, node enters LISTEN state and collects beacon message i.e. HELLO, JOIN, WITHDRAW and executes coverage eligibility rule.

Step3: Beacon messages broadcast by a node 'x' are authenticated using LEAP's one way key chain mechanism.

Step 4: Node 'x' generates a one way key chain of certain length, then transmits the first key(say AUTH Key) of the key chain to its neighbor 'y', using their shared pairwise key Kxy.
x→y:AUTH Key, MAC(Kxy, AUTH Key);

Step5: Neighbor node 'y' computes MAC by taking input as message from 'x' and shared pairwise key Kxy.

Step6: Neighbor 'y' stores AUTHKEY sent by node 'x' only if both MAC's are equal, else discards message sent by node 'x'.

Step7: Neighbor 'y' verifies each message sent by node 'x' based on the key it received from node 'x' previously i.e. node 'x' sends x →y: HELLO, x, pos,K_{x-I};

Note: Keys are disclosed in reverse order.

Step8:If the key is valid, then node 'y' takes information from message sent by node 'x' and decides to go to working or sleep state ,else discards message.

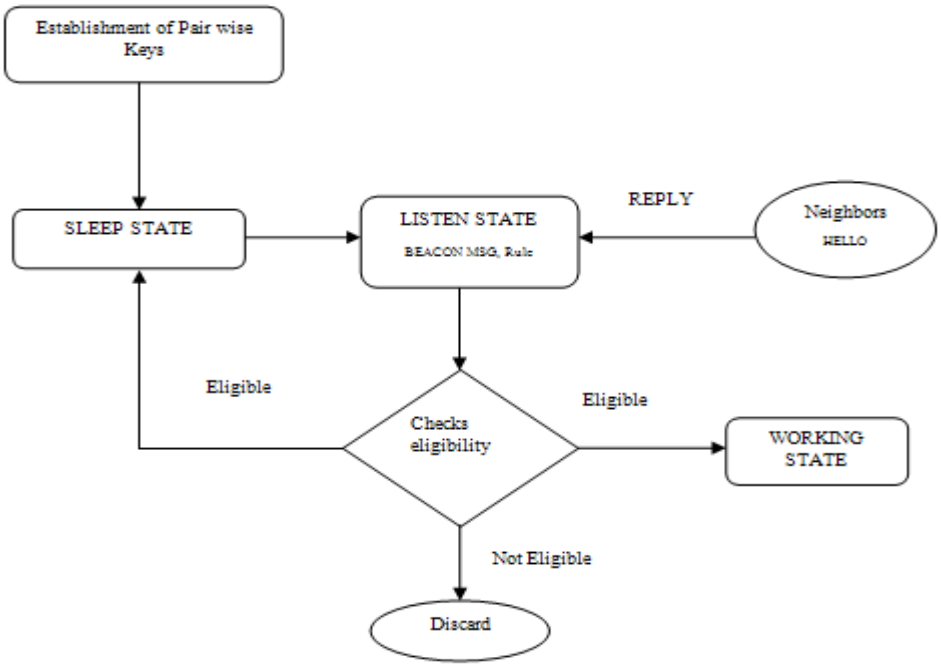

Figure 4: Defensive Measure for CCP

VI. RESULTS AND DISCUSSIONS

In this section, simulations performed for the PEAS protocol and obtained experimental results are described. The goal of the simulation is to study the effects of the countermeasures on the network lifetime and to ensure that the proposed measures do not compromise the stability and performance of the network. Simulation for the CCP protocol is not shown because the proposed countermeasures do not have impact on network connectivity. In the original PEAS protocol, a node makes state transition decisions by taking information from the REPLY's received from its neighbors without performing authentication, while the proposed counter-measures require the node to take information only from authenticated REPLY's. This imposes additional costs for computation, transmission, and memory to store shared pair wise keys of a node , for authentication purpose.

Table 1: Node Parameters for Simulation.

Parameter	Values
Transmission consumption (T_x)	60mW
Reception consumption (R_x)	12mW
Idle consumption	12mW
Sleeping consumption	0.03mW
Initial energy of a node	54 ~ 60 Jules i.e. allowance for a node to operate about 4500 ~ 5000 seconds in reception/idle modes.
Sensing Range (R_S)	10meters
Transmitting Range (R_T)	10meters
Communication Capacity	20Kbps
Size of messages(PROBE,REPLY)	25bytes

PEAS is implemented in PARSEC language, and node parameter values similar to Berkeley Motes are selected, which are summarized in Table1. Nodes are uniformly distributed in an area of 50x50 m^2 and they remain stationary after deployment. The source and the sink are placed in opposite corners of the area, and the source generates 10 data reports per minute. The reports are delivered to the sink

using the GRAB forwarding protocol. The probing range R_P is set to 3 meters, the initial per-node probing rate λ is equal to 0.1 wake up/sec so that the number of working nodes quickly stabilizes. The desired aggregate probing rate λ_d is chosen as 0.02 wake up/sec, that is, each active node should perceive a node wake up every 50 seconds. The node failure rate is set to 10.66 failures/5,000 seconds.

The Coverage Lifetime and Connectivity Lifetime are the metrics used to evaluate the PEAS protocol. The Coverage Lifetime is defined as the time interval from activation of the network until the percentage of the area that is being monitored simultaneously by at least K working nodes, drops below a specified threshold. The Coverage Lifetime characterizes how long the system ensures that interested events are monitored and reported properly. The Connectivity Lifetime is defined as the time interval from activation of the network until the percentage of the reports delivered to the destination, with respect to the total number of reports sent, drops below a specified threshold. The threshold values for both the coverage and connectivity measurements are chosen to be 90 percent, that is, the coverage lifetime ends when the monitored area drops below 90 percent of the total area to be monitored. The connectivity lifetime ends, when the number of reports delivered to the destination drops below 90 percent of the sent reports.

Figure 5 show the performance of PEAS with proposed counter measures for various choices of t, i.e. with several choices of the number of REPLYs. The‘t’ value gives the density of active nodes in the network. More precisely, an adversary has to compromise at least ‘t+1’ nodes within the communication range of ‘x’ to successfully attack node ‘x’.

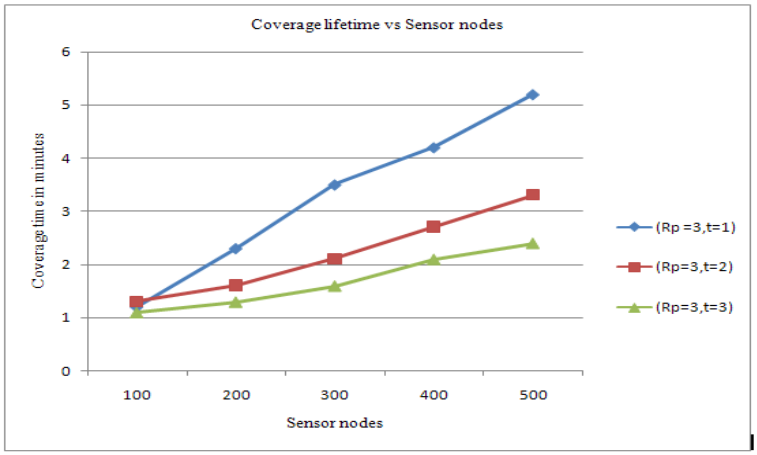

Figure 5: Network coverage lifetime

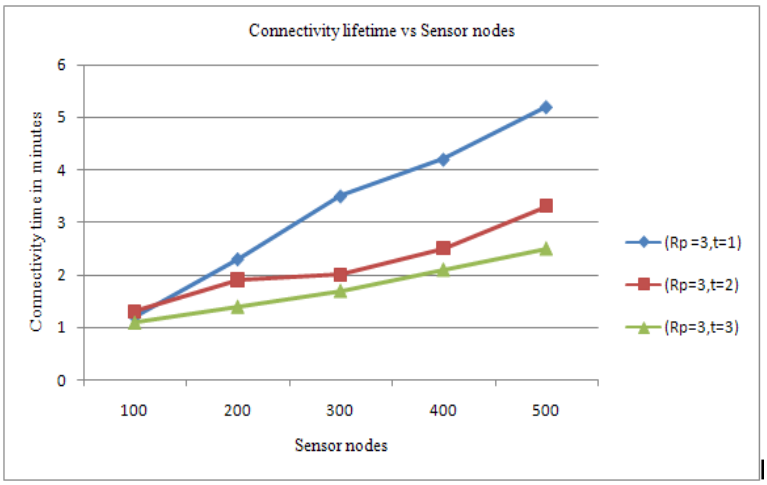

Figure 6 : Network Connectivity Lifetime

In the above graphs, as parameter t increases, the network lifetime is decreased because of the greater number of simultaneous active nodes. As a consequence, the greater the required resilience to adversaries, the smaller the performance of PEAS with proposed measures. For example, when 't' is zero ,the number of REPLYs are equal to 1, the performance of the modified protocol is almost the same as the performance of the original one, the only overhead introduced is cost for computation of MAC to authenticate exchanged messages.

On the contrary, the increase in the number of simultaneous active nodes that are introduced with the countermeasures improves network performance on data delivery. The number of simultaneously active nodes in PEAS is determined by the value of R_P and t, while the protocol resilience to attackers is only determined by t. Therefore choose a greater value of R_P in order to increase the lifetime of the network that adopts PEAS with proposed measures, while keeping 't' value unchanged.

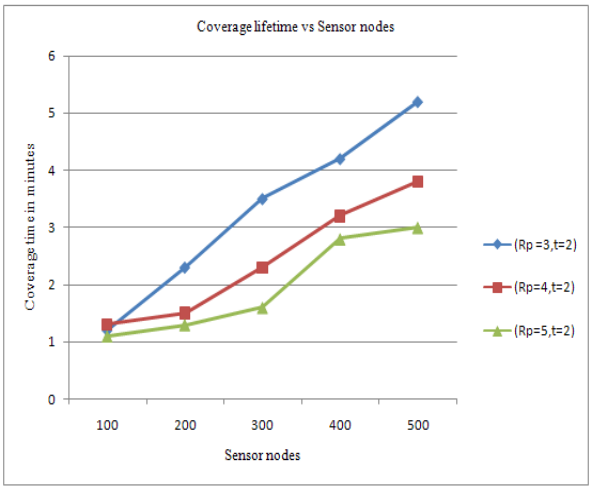

Figure 7: Network coverage lifetime with increasing Rp value.

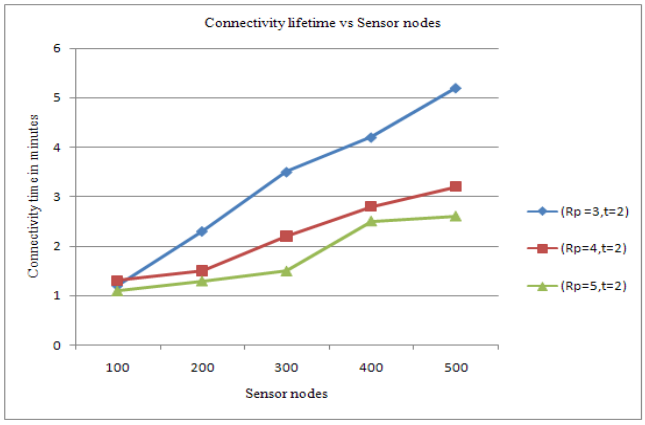

Figure 8: Network Connectivity lifetime with increasing Rp value.

Figure 7 and Figure 8, confirms to increase in sensing coverage lifetime and network lifetime when R_P is increased, without compromising stability of network.

VII. CONCLUSION & FUTURE WORK

In this paper, topology maintenance protocols crucial for the operation of wireless sensor networks and attacks against these protocols have been analyzed. The defensive measures proposed ensure authenticated communication between a node and its neighbor nodes. These defensive measures include shared pair wise keys to generate MAC, and LEAP's one way key chain mechanism to authenticate messages being exchanged. This enables a node to make correct decisions based on the information in authenticated messages received from its neighbor nodes, thus detection and avoidance of impersonation attacks in the network is achieved, thereby increased robustness of

protocols is also achieved which guarantees enhanced functionality of sensor application. Future work includes periodic check of state transition decisions by topology maintenance protocols, where the eligibility of node to be in active or sleep state will be checked periodically.

REFERENCES

[1]. Gabrielli, L.V. Mancini, S. Setia, and S. Jajodia, "Securing Topology Maintenance Protocols for Sensor Networks: Attacks and Countermeasures," Proc. First IEEE Int'l Conf. Security and Privacy for Emerging Areas in Comm. Networks (SecureComm '05), Sept. 2005.

[2]. F. Ye, G. Zhong, S. Lu, and L. Zhang, "PEAS: A Robust Energy Conserving Protocol for Long-Lived Sensor Networks," Proc. 23rd IEEE Int'l Conf. Distributed Computing System (ICDCS '03), May 2003.

[3]. Shuo Zhang , Yuheng Liu, Juhua Pu, Xiao Zeng, Zhang Xiong "An Enhanced Coverage Control Protocol for Wireless Sensor Networks", Proc. 42nd IEEE Int'l Conf.System Sceinces,2009.

[4]. S. Zhu, S. Setia, and S. Jajodia, "LEAP: Efficient Security Mechanisms for Large-Scale Distributed Sensor Networks," Proc.10th ACM Int'l Conf. Computer and Comm. Security (CCS'03), citeseer.ist.psu.edu/zhu03leap.html, Oct. 2003.

[5]. Parno, A. Perrig, and V. Gligor, "Distributed Detection of Node Replication Attacks in Sensor Networks," Proc. IEEE Symp. Security and Privacy (S&P '05), May 2005.

[6]. W. Xu, K. Ma, W. Trappe, and Y. Zhang, "Jamming Sensor Networks: Attack and Defense Strategies," IEEE Networks Special Issue on Sensor Networks, vol. 20, no. 3, pp. 41-47, May/June 2006.

[7]. Y. Zhang, W. Lee, and Y.-A. Huang, "Intrusion Detection Techniques for Mobile Wireless Networks," ACM Wireless Networks,vol. 9, no. 5, pp. 545-556, Sept. 2003.

[8]. Akyildiz, I.F., W. Su, Y. Sankarasubramaniam, and E.Cayirci, A survey on sensor networks, IEEE Communications Magazine, 40(8): pp. 102-105, 2002.

AUTHORS

Barigala Lydia Sravanthi was born in 1989 in India. She received B.Tech degree in Computer Science and Engineering from Jawaharlal Nehru Technological University in India in 2010. She is currently pursuing M.Tech in Computer Science and Engineering from Jawaharlal Nehru Technological University in India.

Yaramati Sarada Devi was born in 1986 in India. She received M.Tech degree in Computer Networks and Information Security from School of Information Technology, Jawaharlal Nehru Technological University in India in 2009.She received B.Tech degree in Computer Science and Engineering from Jawaharlal Nehru Technological University in India in 2007.She is currently working as Assistant Professor in CMR College of Engineering and Technology in Hyderabad, India.

Pulabam Soujanya was born in 1983 in India. She received M.Tech degree in Computer Science and Engineering from Jawaharlal Nehru Technological University in India in 2011.She received B.Tech degree in Computer Science and Engineering from Jawaharlal Nehru Technological University in India in 2005.She is currently working as Assistant Professor in CMR College of Engineering and Technology in Hyderabad, India.

T. Dharma Reddy was born in India. He is currently working as Assistant Professor in CMR College of Engineering and Technology in Hyderabad, India.