Asian Journal of Information Technology 11 (6-12): 285-292, 2012
ISSN: 1682-3915

Secure Authentication Technique for Localization in Wireless Sensor Networks

[1, 2]P.S. Velumani and [3]S. Murugappan
[1]Educational and Research Institute University, Chennai, India
[2]Model Institute of Engineering and Technology, Jammu, India
[3]Department of Computer Science and Engineering, Annamalai University, Chennai, India

Abstract: In Wireless Sensor Networks (WSN), the secure localization is extremely significant for enhancing the accuracy of localization and robustness against security threats. Also most the existing literature research lacks the security approach towards localization mechanism which may affect the secure communication of the data. Hence, in this study, researchers propose a secure authentication technique for localization in WSN. Initially the position of sensor nodes is estimated using proximity distance map computation. The anchor nodes then generate a location based key pair for each sensor node. This ensures that the attackers cannot exploit the positions and location based keys of compromised nodes. Then, the mutual authentication of neighbour nodes is performed based on location information. By simulation results we show that the proposed approach offers improved security in WSN.

Key words: Secure Walking GPS (SWG), Ant Colony Optimization (ACO), Secure Authentication Technique for Localization in WSN (SATL), India

INTRODUCTION

Wireless sensor networks: Smart environments represent the next evolutionary development step in building, utilities, industrial, htransportation systems automation. A wireless sensor network is a collection of nodes organized into a cooperative network. Each node consists of processing capability may contain multiple types of memory (program, data and flash memories) have a RF transceiver (usually with a single omnidirectional antenna) have a power source and accommodate various sensors and actuators. The nodes communicate wirelessly and often self organize after being deployed in an ad hoc fashion. Systems of 1000s or even 10,000 nodes are anticipated. Such systems can revolutionize the way researchers live and work (Stankovoic, 2006; Lewis, 2004; Akyildiz *et al*., 2002).

Currently, wireless sensor networks are beginning to be deployed at an accelerated pace. It is not unreasonable to expect that in 10-15 years that the world will be covered with wireless sensor networks with access to them via the internet. This can be considered as the internet becoming a physical network. This new technology is exciting with unlimited potential for numerous application areas including environmental, medical, military, transportation, entertainment, crisis management, homeland defense and smart spaces. A sensor network is composed of a large number of sensor nodes which are densely deployed either inside the phenomenon or very close to it. The sensors in a node observe phenomena such as thermal, optic, acoustic, seismic and acceleration events while the processing and other components analyze the raw data and formulate answers to specific user requests. The recent advances in technology mentioned earlier have paved the way for the design and implementation of new generations of sensor network nodes, packaged in very small and inexpensive form factors with sophisticated computation and wireless communication abilities (Lewis, 2004; Stankovoic, 2006).

Once deployed, sensor nodes begin to observe the environment, communicate with their neighbours (i.e., nodes within communication range), collaboratively process raw sensory inputs and perform a wide variety of tasks specified by the applications at hand. The key factor that makes wireless sensor networks so unique and promising both in terms of research and economic potentials is their ability to be deployed in very large scales without the complex pre planning, architectural engineering and physical barriers that wired systems have faced in the past.

For wireless sensor networks, the systems are wireless have scarce power are real time, utilize sensors and actuators as interfaces have dynamically changing sets of resources, aggregate behaviour is important and location is critical. Many wireless sensor networks also utilize minimal capacity devices which places a further strain on the ability to use past solutions (Stankovoic, 2006; Akyildiz *et al*., 2002).

Corresponding Author: P.S. Velumani, Educational and Research Institute University, Chennai, India

Security in wireless sensor networks: A wireless sensor network is a special network which has many constraints compared to a traditional computer network. Because sensor networks pose unique challenges, traditional security techniques used in traditional networks cannot be applied directly. Unlike traditional networks, sensor nodes are often deployed in accessible areas, presenting the added risk of physical attack. Sensor networks interact closely with their physical environments and with people, posing new security problems. Due to these constraints it is difficult to directly employ the existing security approaches to the area of wireless sensor networks (Karlof and Wagner, 2003; Boyle and Newe, 2008).

Securing the Wireless Sensor Network needs to make the network support all security properties: confidentiality, integrity, authenticity and availability. Attackers may deploy a few malicious nodes with similar hardware capabilities as the legitimate nodes that might collude to attack the system cooperatively. The attacker may come upon these malicious nodes by purchasing them separately or by turning a few legitimate nodes by capturing them and physically overwriting their memory (Kalita and Kar, 2009; Kellner *et al*., 2012).

Basic security requirements in WSNs: A sensor network is a special type of network. It shares some commonalities with a typical computer network but also poses unique requirements of its own. To achieve secure routing in WSNs there are several basic security requirements that should be taken into account (Fig. 1) such as confidentiality, integrity, authentication, authorization/access control, availability, robustness, freshness and secrecy (Kellner *et al*., 2012).

Many sensor network routing protocols are quite simple. The most popular types of attacks are: denial of service attacks, sybil attack, traffic analysis attack, node replication attack, attacks against privacy, physical attacks, spoofed, altered or replayed routing information, selective forwarding, sinkhole attacks, wormholes, HELLO flood attacks, acknowledgement spoofing. These are the Attacks on Wireless Sensor Network routing (Karlof and Wagner, 2003; Kellner *et al*., 2012).

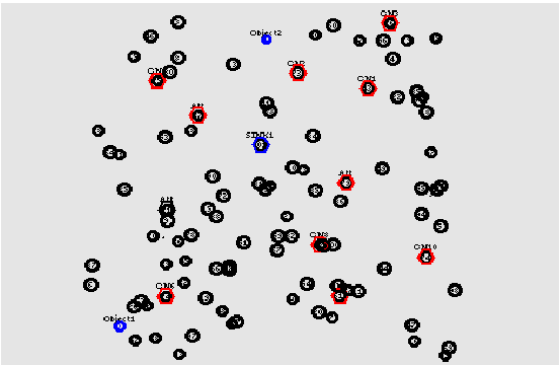

Fig. 1: Simulation topology

To improve the security of routing protocols in WSNs, various security measures can be applied. Although, most of the concepts are well known concepts that were used in other areas of computer science for years, the special characteristics of WSNs have to be considered when applying them in WSNs. Cryptography, symmetric cryptography, public key cryptography, hybrid cryptography, energy consumption, data aggregation existing secure routing protocols for WSNs are used to measuring the secure routing in WSN's (Kellner *et al*., 2012).

Localization in wireless sensor network: Location awareness is important for wireless sensor networks since, many applications such as environment monitoring, vehicle tracking and mapping depend on knowing the locations of sensor nodes. The localization problem has received considerable attention in the past as many applications need to know where objects or persons are and hence various location services have been created. Undoubtedly, the Global Positioning System (GPS) is the most well known location ser ice in use today. Since, most applications depend on asuccessful localization, i.e., to compute their positions in some fixed coordinate system it is of great importance to design efficient localization algorithms (Hu and Evans, 2004; Langendoen and Reijers, 2003; Pal, 2010).

There are three important metrics associated with localization: energy efficiency, accuracy and security. Though the first two metrics have been researched extensively, the security metric has drawn the attention of researchers only recently and as such has not been addressed adequately. Measurement techniques in WSN localization can be broadly classified into three categories: AOA measurements distance related measurements and RSS profiling techniques (Mao and Fidan, 2009; Srinivasan and Wu, 2007).

Attacks on localization: Some attacks that have been discussed for nearly a decade in literature that are the most common against localization schemes are as follows.

Replay attack: A replay attack is the easiest and most commonly used by attackers. Specifically when an attacker's capability is limited, i.e., the attacker cannot compromise more than one node; this is the most preferred attack. In a replay attack, the attacker merely jams the transmission between a sender and a receiver and later replays the same message posing as the sender.

Sybil attack: The sybil attack requires a more sophisticated attacker compared to the replay attack. In a sybil attack, a node claims multiple identities in the network. When launched on localization, localizing nodes can receive multiple location references from a single node leading to incorrect location estimation.

Wormhole attack: In a wormhole attack, an attacker obtains two transceivers in the network connected by a high quality out of band link and replays messages heard at one location at the other location. A wormhole attack can easily disrupt existing localization techniques even if all location announcements were successfully encrypted (Srinivasan and Wu, 2007; Hu and Evans, 2004).

Need for secure localization: Secure localization is very important in wireless sensor networks because to improve the accuracy of localization and robustness against security threats. To improve the accuracy of localization researchers have to filtering false information which may also influence the frequency of false positives and false negatives inverification scheme. Security in WSN becomes very important due to the attacks. Researchers have adopt the new secure localization schemes to get protection from these attacks (Langendoen and Reijers, 2007).

Problem identification: In study Velumani and Murugappan (2012), a target tracking and localization technique based on the ant colony optimization with the help of anchor nodes has been proposed. Initially a set of anchor nodes are deployed using the distance between the nodes. The ant based routing protocol is used to find the best route with the shortest hop distance by acquiring the proximity information between every pair of anchor nodes. When a sensor node detects the target, the localization process is carried out using the anchor nodes and the position of the target is tracked using ant agents and the gathered information is transmitted to the sink. The earlier approach lacks secure communication between the sensor nodes and anchor nodes so, the attacker will compromise the sensor node. So, as an extension to this researchers propose to design a secure authentication technique for localization in MANET.

LITERATURE REVIEW

Mi *et al.* (2010) have proposed a secure walking GPS, a secure localization and key distribution solution for manual deployments of WSNs. Using the location information provided by the GPS and inertial guidance modules on a special master node, secure walking GPS achieves accurate node localization and location based key distribution at the same time. They presented the design and evaluation of secure walking GPS, an integral solution for secure localization and location based key distribution in large scale and manually deployed WSNs. Secure walking GPS is practical and low cost, requires minimal human interaction during the deployment and makes the deployed WSN resistant to the Dole Yao, the wormhole and the GPS denial attacks.

Liu *et al.* (2008) have proposed two types of attack resistant location estimation techniques to tolerate the malicious attacks against range based location discovery in wireless sensor networks. The first technique, named Attack Resistant Minimum Mean Square Estimation (ARMMSE) is based on the obser ation that malicious location references introduced by attacks are intended to mislead a sensor node about its location and thus are usually inconsistent with the benign ones. The first method filters out malicious beacon signals on the basis of the consistency among multiple beacon signals while the second method tolerates malicious beacon signals by adopting an iteratively refined voting scheme. Both methods can survive malicious attacks even if the attacks bypass authentication, provided that the benign beacon signals constitute the majority of the beacon signals.

Chen *et al.* (2008) have proposed TSCD secure localization to overcome the distance consistent spoofing attack in wireless sensor networks. The main idea of the TSCD scheme is to firstly apply the temporal and spatial properties of locators to detect some attacked locators and then utilize the consistent properties of the attacked locators and legitimate locators to find out other attacked locators. Simulation results demonstrate that the proposed scheme achieves better performance than existing approaches under the same network parameters. The main contributions of this researchers are summarized as follows: they first summarize four secure properties of locators under the distance consistent spoofing attack they propose the TSCD secure localization scheme to yield good performance under the presence of the distance consistent spoofing attack; they analyze the effects of network parameters to the performance and compare the scheme with existing methods.

Chen *et al.* (2009) have proposed a wormhole attack resistant secure localization scheme. The main idea of the proposed scheme is to build a so called conflicting set for each locator based on the abnormalities of message exchanges among neighbouring locators and then to identify all dubious locators which are filtered out during localization. Their proposed scheme can identify the dubious locators with a very high probability to achieve secure localization. The main idea of their proposed

scheme is to build a so called conflicting set for each locator based on the abnormalities of message exchanges among neighbouring locators and then identify all the dubious locators which can be filtered out during localization.

Chen *et al.* (2010) have proposed a secure localization scheme against wormhole attacks which includes three phases: wormhole attack detection, neighbouring locator's differentiation and secure localization. The main idea of the proposed secure localization scheme is to build a so called conflicting set for each locator according to the abnormalities of message exchanges among neighbouring locators which is used to differentiate the dubious locators from alid locators for the secure localization. A potential solution is to separate the localization from the wormhole attack detection. That is when multiple wormhole attacks are detected, the system can try to identify the locations of the attackers and then eliminate them. Thus, the other direction of the future research will focus on the detection of multiple wormhole attacks and the localization of the attackers.

PROPOSED RESEARCH

Overview: In this study, researchers propose to design a secure authentication technique for localization in MANET. In this technique, initially the sensor node position is estimated using proximity distance map. After estimating the positions of normal sensor nodes, the anchor nodes compute a location based key pair for each node. Then, it creates a hash and encrypts this key pair and sends it to each sensor nodes. On receiving it each sensor in turn can decrypt and authenticate the message. Then, mutual authentication of neighbour nodes is performed based on location information.

Proposed technique: The proposed technique uses location based keys in securing communication among the sensor and the anchor nodes. This approach also, authenticates the neighbours of the respective nodes. It involves two phases. In the first phase, the position of normal sensor nodes is estimated. The second phase involves location based key generation and authentication technique.

Phase-1 (Estimating the position of the normal sensor node): Initially, an Ant Colony Optimization (ACO) technique is used for the route discovery process. Each object creates a set of routing agents called FANT (Forward ANT) and Backward Ants (BANT) to search for the route to anchor node. In route discovery mechanism, the source will disseminate FANT to all its one-hop neighbours when a path to the anchor node is to be established. While the anchor node is still not found, the neighbour would keep forwarding the FANTs to their own neighbours and so on. At the end of this route discovery mechanism, the routing table for each node contains the optimum path between the selected anchor nodes.

The routing protocol used for route discovery is concerned with finding the best route using ant colony optimization. In order to increase the co erage of the network, the shortest hop distance is calculated by acquiring the proximity information between every pair anchor nodes.

After calculating the shortest path distance using the ANT agents all the anchor nodes gets the information about the position estimates of the each other. MDS provides a configuration about the anchor nodes. Thus, the proximity distance map T among the anchor nodes can be calculated immediately.

Proximity Distance Map (PDM) calculation: Researchers create two matrix tables: Proximity matrix contain the information about the hop count between the anchors. Geographical distance matrix contains the position estimates obtained from the Proximity matrix.

Let F be the proximity matrix that fxy is the proximity measure between anchors x and y where fxy = 0. The proximity measure can be hop count or cumulative path distance between anchors. Similarly, let G be a geographical distance matrix that gxy is the geographical distance between anchors x and y. The gxy can be calculated by utilizing the position estimates obtained from the previous step. The L and G are square matrices with size v, v where v is the total number of anchors. The PDM J is the linear mapping that maps matrix F to matrix G and the following error is minimized:

$$Q = ||fiJ\text{-}riF||2 \quad (1)$$

Where:

fi = fi1, ... fim

J and ri = The ith row of J

$$J = FGJ\ (GGJ)\text{-}1 \quad (2)$$

Localization of normal nodes: Each normal sensor node (S) uses the mapping J to process the proximity vector vs it has stored when it aided anchors exchanging proximity information:

$$X_s = J_{vs} \quad (3)$$

Finally, the node position is calculated by multilateration with the processed proximity vector and the position information of primary and secondary anchors (Velumani and Murugappan, 2012).

Phase-2 (Security mechanism)

Estimation of secret key (K_{sec}): K_{sec} is assigned to each sensor node by TA before they are deployed in the network. It is estimated using following equation:

$$K_{sec} = h_k (ID_i) \quad (4)$$

Where:

ID_i = Sensor nodes ID
h = Hash function
h_k = Message integrity code of message (m) protected by key K

Secure authentication technique: This technique enhances the security and survivability of sensor nodes of the network. The steps involved in this mechanism are as follows:

- Assigning the pairing parameters to sensor and anchor nodes
- Generating the location based keys
- Mutual authentication of neighbour nodes based on location

Assigning the pairing parameters to sensor and anchor nodes: Researchers take ID Based Cryptography (IBC) technique into consideration which is otherwise called as pairing technique. This helps in deriving the public keys of entities from their respective publicly identified identity information. It avoids the necessity of distributing the authenticated public key through public key certificates.

Let A_1 and A_2 represent the additive cyclic group and multiplicative cyclic group of prime order y. Consider that the Discrete Logarithm Problem (DLP) is complex in both A_1 and A_2.

A pairing is defined as a bilinear map $\hat{b}$ such that $A_1 \times A_1 \rightarrow A_2$. If all U, V, W, X$\epsilon$ A_1 then:

$$\hat{b}(U+V, W+X) = \hat{b}(U,W)\,\hat{b}(U,X)\,\hat{b}(V,W)\,\hat{b}(V,X) \quad (5)$$

The Trusted Authority (TA) assigns the pairing parameters (y, A_1, A_2, $\hat{b}$) to sensor nodes before they are deployed in the network. These nodes choose a random number f ϵ Z^*_y. This is referred to as master key (K_M).

Also node selects a cryptographic hash function h which maps the arbitrary strings to non zero elements in A_1. Though, both sensor and anchor nodes are pre loaded with pairing parameters (y, A_1, A_2, $\hat{b}$, h) only anchors have the knowledge of f.

Generating the location based keys: Following the above parameter loading process, the location of the sensor nodes (X_S) are estimated. Then the anchor nodes generates location based key (K_L) for sensor nodes using following equation:

$$K_L = f\,h_k (X_S) \quad (6)$$

Then, the anchor node transmits a message Z to S:

$$AN \rightarrow S: Z$$

The format of Z is as follows:

$$Z = \{X_S, K_L, h_k (X_S \| K_L)\}K_{sec} \quad (7)$$

Where:

$\{X_S, K_L\}$ = Public/private key pair of S
K_{sec} = Secret key

Subsequently, S decrypts the message and authenticates it over again. As DLP is complex in A1, it is difficult to deduce f from any given $\{X_S, K_L\}$ pair. This means that even though an random number of sensor nodes are compromised, attackers however cannot exploit the positions and location based keys of compromised nodes to derive f.

Mutual authentication of neighbour nodes based on location: The mutual authentication algorithm is as follows:

Consider two neighbour nodes S and T.

Step 1: S broadcasts its location X_S and random nonce g_S to its neighbour nodes within the transmission range R_{tx}:

$$S \rightarrow^* \{X_S, g_S\}$$

Step 2: When the neighbour node T receives the broadcast message, it verifies whether the declared location is within R_{tx}. The verification is done using the following condition:

$$\text{if } (X_S - X_T) \leq R_{tx}$$

Then

T computes $K_{S,T}$ (in Eq. 8)

$$T \xrightarrow{\{X_S, g_S, \lambda\}} S$$

Else

T neglects the authentication message.

End if

where, $K_{S,T}$ is shared pair wise key and is computed using the following equation:

$$K_{S,T} = e(K_{LS}, h(X_T) = e(fh(X_S), h(X_T) \quad (8)$$

$$\lambda = h K_{S,T}(g_S \| g_T \| 1) \quad (9)$$

Step 3: S upon receiving the message from T verifies the following condition:

$$\text{if } (X_S - X_T) \leq R_{tx}$$

Then
S computes $K_{T,S}$ (in Eq. 10):

$$S \xrightarrow{(\delta)} T$$

End if

$$K_{T,S} = e(h(X_S), KL_T) = e(h(X_S), f h(X_T) \quad (10)$$

$$\delta = h K_{S,T}, (g_S \| g_T \| 2) \quad (11)$$

Step 4: $K_{S,T}$ and $K_{T,S}$ estimated in Step 3 and 4 are said to be equal only when S contains authentic K_S and T holds the authentic K_T. Hence,

If λ matches with the alue computed by S

Then

S considers T to be authenticated neighbour.

End if

Similarly
If δ matches with the value computed by T

Then

T considers S to be authenticated neighbour.

End if

Step 5: Using the earlier steps, the remaining nodes also performs mutual authentication.

SIMULATION RESULTS

Simulation parameters: The Secure Authentication Technique for Localization (SATL) is evaluated through Network Simulator (NS2). Researchers use a bounded region of 500×500 sqm in which 100 sensor nodes are randomly placed and a sink node is located in the center of the network. Researchers have used two target objects which randomly move across the network whose location information has to be tracked by the sensor nodes.

The power levels of the nodes are assigned such that the transmission range and the sensing range of the nodes are all 250 m. In the simulation, the channel capacity of mobile hosts is set to the same value: 2 Mbps. The simulated traffic is Constant Bit Rate (CBR). The simulation topology is given in Fig. 1. Table 1 summarizes the simulation parameters used.

Table 1: Simulation settings

Parameters	Target
No. of nodes	100
Area size	500×500
Mac	802.11
Simulation time	50 sec
Traffic source	CBR
Packet size	512
Transmit power	0.360 W
Receiving power	0.395 W
Idle power	0.335 W
Initial energy	12.1 J
Transmission range	250, 300, 350, 400 and 450 m
Routing protocol	SATL
Attackers	1, 2, 3, 4 and 5

Performance metrics: The performance of the proposed SATL technique is compared with the SWG (Mi *et al*., 2010) Method. Researchers evaluate mainly the performance according to the following metrics.

Average energy consumption: The average energy consumed by the nodes in receiving and sending the packets.

Packet delivery ratio: It is defined as the number of data packets received successfully with the total number of packets sent.

Average end to end delay: It includes the localization delay, tracking delay and transmission delay.

EXPERIMENTAL RESULTS

Based on transmission range: From Fig. 2, researchers can see that the delay of the proposed SATL is less than the existing SWG Method. From Fig. 3, researchers can see that the delivery ratio of the proposed SATL is higher than the existing SWG Method. From Fig. 4, researchers can see that the energy consumption of the proposed SATL is less than the existing SWG Method.

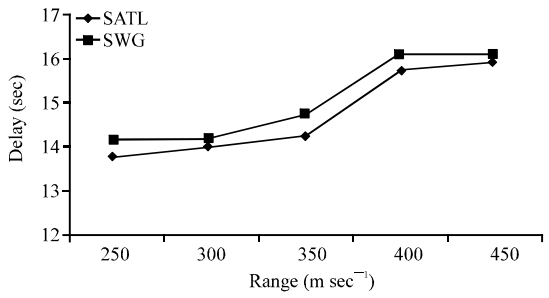

Fig. 2: Range vs. delay

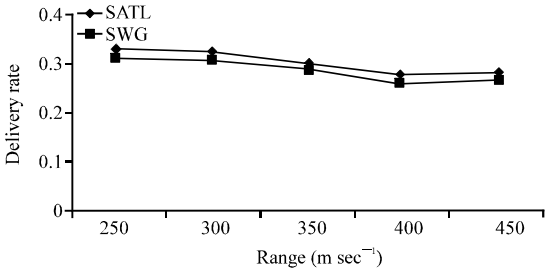

Fig. 3: Range vs. delivery ratio

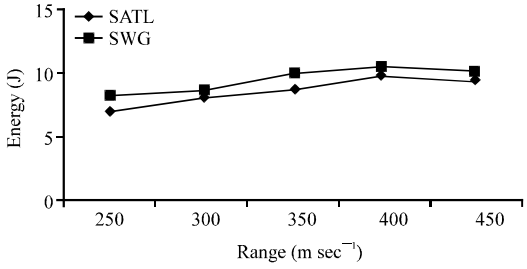

Fig. 4: Range vs. energy

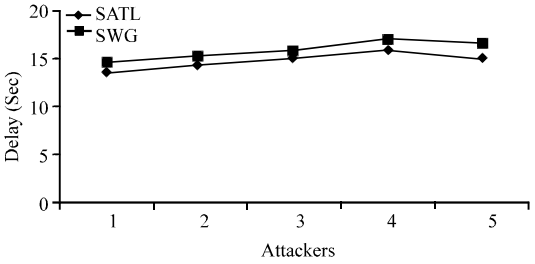

Fig. 5: Attackers vs. delay

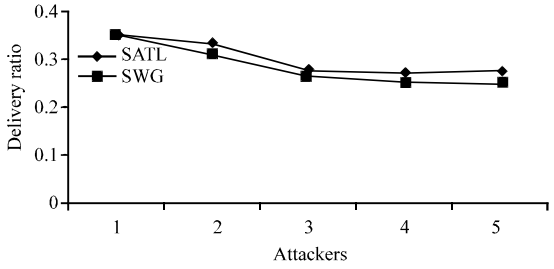

Fig. 6: Attackers vs. delivery ratio

Based on attackers: In the second experiment researchers vary the number of attackers as 1-5. From Fig. 5, researchers can see that the delay of the proposed SATL is less than the SWG Method.

From Fig. 6, researchers can see that the delivery ratio of the proposed SATL is higher than the existing SWG Method. From Fig. 7, researchers can see that the energy consumption of the proposed SATL is less than the existing SWG Method.

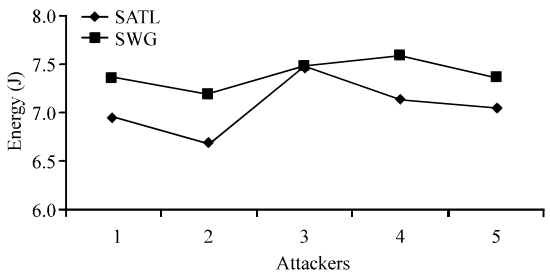

Fig. 7: Attackers vs. energy

CONCLUSION

In this study, researchers have proposed a secure authentication technique fir localization in WSN. Initially the position of sensor nodes is estimated using proximity distance map computation. The anchor nodes then generate a location based key pair for each sensor node. This ensures that the attackers cannot exploit the positions and location based keys of compromised nodes. Then the mutual authentication of neighbour nodes is performed based on location information. By simulation results, researchers have shown that the proposed approach offers improved security in WSN. The main advantage of this approach is that though some random count of sensor nodes are compromised, the attackers cannot reveal or find the location and keys of compromised nodes and hence location based keys of compromised nodes cannot be generated.

ACKNOWLEDGEMENT

Researchers thankful to Director Dr. Ankur Gupta, Model Institute of Engineering and Technology, Jammu, Convener Research and Publication Cell for the encouragement, motivation and support.

REFERENCES

Akyildiz, I.F., W. Su, Y. Sankarasubramaniam and E. Cayirci, 2002. Wireless sensor networks: A survey. Comput. Networks, 38: 393-422.

Boyle, D. and T. Newe, 2008. Securing wireless sensor networks: Security architectures. J. Networks, 3: 65-77.

Chen, H., W. Lou and Z. Wang, 2009. Conflicting-set-based wormhole attack resistant localization in wireless sensor networks. Proceedings of the 6th International Conference on Ubiquitous Intelligence and Computing, July 7-9, 2009, Brisbane, Australia, pp: 296-309.

Chen, H., W. Lou and Z. Wang, 2010. Secure localization against wormhole attacks using conflicting sets. Proceedings of the IEEE 29th International Performance Computing and Communications Conference, December 9-11, 2010, Albuquerque, NM., USA., pp: 25-33.

Chen, H., W. Lou, J. Ma and Z. Wang, 2008. TSCD: A novel secure localization approach for wireless sensor networks. Proceedings of the 2nd International Conference on Sensor Technologies and Applications, August 25-31, 2008, Cap Esterel, France, pp: 661-666.

Hu, L. and D. Evans, 2004. Localization for mobile sensor networks. Proceedings of the 10th Annual International Conference on Mobile Computing and Networking, September 26-October 1, 2004, Philadelphia, USA., pp: 45-57.

Kalita, H.K. and A. Kar, 2009. Wireless sensor network security analysis. Int. J. Next Gener. Networks, 1: 1-10.

Karlof, C. and D. Wagner, 2003. Secure routing in wireless sensor networks: Attacks and countermeasures. J. Ad Hoc Networks, 1: 293-315.

Kellner, A., O. Alfandi and D. Hogrefe, 2012. A Survey on measures for secure routing in wireless sensor networks. Int. J. Sensor Networks Data Communi., 1: 1-17.

Langendoen, K. and N. Reijers, 2003. Distributed localization in wireless sensor networks: A quantitative comparison. Int. J. Comput. Telecommuni. Networking, 43: 499-518.

Lewis, F.L., 2004. Wireless Sensor Networks. In: Smart Environments: Technologies, Protocols and Applications, Cook, D.J. and S.K. Das (Eds.). John Wiley, New York, ISBN-13: 9780471686583, pp: 13-44.

Liu, D., P. Ning, A. Liu, C. Wang and W.K. Du, 2008. Attack-resistant location estimation in wireless sensor networks. ACM Trans. Inf. Syst. Sec. (TISSEC), Vol. 11. 10.1145/1380564.1380570

Mao, G. and B. Fidan, 2009. Localization Algorithms and Strategies for Wireless Sensor Networks. Idea Group, USA Pages: 510.

Mi, Q., J.A. Stankovic and R. Stoleru, 2010. Secure walking GPS: A secure localization and key distribution scheme for wireless sensor networks. Proceedings of the 3rd ACM Conference on Wireless Network Security, March 22-24, 2010, Hoboken, NJ, USA., pp: 163-168.

Pal, A., 2010. Localization algorithms in wireless sensor networks: Current approaches and future challenges. Network Protocols Algorithms, 2: 45-73.

Srinivasan, A. and J. Wu, 2007. A Survey on Secure Localization in Wireless Sensor Networks. In: Wireless and Mobile Communications, Furht, B. (Ed.). CRC Press, Boca Raton, London.

Stankovoic, J.A., 2006. Wireless sensor networks. University of Virginia, Charlottesville, VA., USA.

Velumani, P.S. and S. Murugappan, 2012. Ant based target tracking and localization technique for wireless sensor networks. Eur. J. Sci. Res., 70: 554-568.