ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 2, February 2015

Vampire Attack Detection in Wireless Sensor Networks

S. Jayashree[1], T.Mohanraj [2]

III M.E., Dept of CSE, Karpagam University, Coimbatore , India[1]

Assistant Professor, Dept of CSE, Karpagam University, Coimbatore , India[2]

ABSTRACT*:* Secure Data transmission is a critical issue for wireless sensor networks (WSNs). Clustering is an effective and practical way to enhance the system performance of WSNs. A secure data transmission for cluster-based WSNs (CWSNs), where the clusters are formed dynamically and periodically. Two Secure and Efficient data Transmission (SET) protocols for CWSNs, called SET-IBS and SET-IBOOS, by using the Identity-Based digital Signature (IBS) scheme and the Identity-Based Online/Offline digital Signature (IBOOS) scheme, respectively. In SET-IBS, security relies on the hardness of the Diffie-Hellman problem in the pairing domain. SET-IBOOS further reduces the computational overhead for protocol security, which is crucial for WSNs, while its security relies on the hardness of the discrete logarithm problem. The feasibility of the SET-IBS and SET-IBOOS protocols with respect to the security requirements and security analysis against various attacks. The calculations and simulations are provided to illustrate the efficiency of the proposed protocols. It improves the security overhead and the energy consumption.

KEYWORDS: PLGP , WSN , vampire attack , VANET

I. INTRODUCTION

The more modern networks are bi-directional, also enabling control of sensor activity. The development of wireless sensor networks was motivated by military applications such as battlefield surveillance; today such networks are used in many industrial and consumer applications, such as industrial process monitoring and control, machine health monitoring. The WSN is built of "nodes" – from a few to several hundreds or even thousands, where each node is connected to one (or sometimes several) sensors. Each such sensor network node has typically several parts: a radio transceiver with an internal antenna or connection to an external antenna, a microcontroller, an electronic circuit for interfacing with the sensors and an energy source, usually a battery or an embedded form of energy harvesting. A sensor node might vary in size from that of a shoebox down to the size of a grain of dust, although functioning "motes" of genuine microscopic dimensions have yet to be created. The cost of sensor nodes is similarly variable, ranging from a few to hundreds of dollars, depending on the complexity of the individual sensor nodes. Size and cost constraints on sensor nodes result in corresponding constraints on resources such as energy, memory, computational speed and communications bandwidth. The topology of the WSNs can vary from a simple star network to an advanced multi-hop wireless mesh network A wireless sensor network (WSN) is increasingly being envisioned for collecting data, such as physical or environmental properties, from a geographical region of interest. WSNs are composed of a large number of low cost sensor nodes, which are powered by portable power sources, e.g. batteries .

In many surveillance applications of WSNs, tracking a mobile target (e.g., a human being or a vehicle) is one of the main objectives. Unlike detection that studies discrete detection events a target tracking system is often required to ensure continuous monitoring, i.e., there always exist nodes that can detect the target along its trajectory (e.g., with low detection delay or high coverage level). Since nodes often run on batteries that are generally difficult to be recharged once deployed, energy efficiency is a critical feature of WSNs for the purpose of extending the network lifetime. However, if energy efficiency is enhanced, the quality of service (QoS) of target tracking is highly likely to be negatively influenced. For example, forcing nodes to sleep may result in missing the passing target and lowering the tracking coverage. Therefore, energy efficient target tracking should improve the trade off between energy efficiency and tracking performance e.g., by improving energy efficiency at the expense of a relatively small loss on tracking performance.

As a compensation for tracking performance loss caused by duty cycling and sleep scheduling, proactive wake-up has been studied for awakening nodes proactively to prepare for the approaching target. However, most existing efforts about proactive wake-up simply awaken all the neighbor nodes in the area, where the target is expected to arrive, without any differentiation. In fact, it is sometimes unnecessary to awaken all the neighbor nodes. To sleep-schedule nodes precisely, so as to reduce the energy consumption for proactive wake-up. For example, if nodes know the exact route of a target, it will be sufficient to awaken those nodes that cover the route during the time when the target is expected to traverse their sensing areas.

II. RELATED WORK

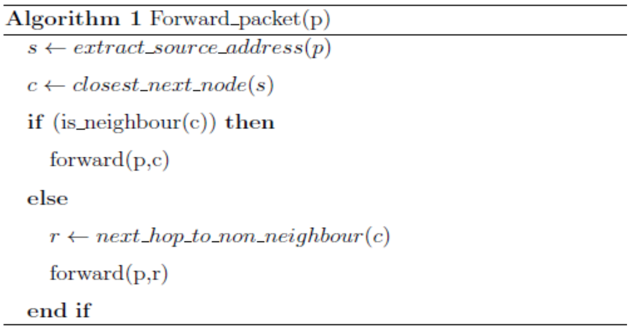
In [1] author presented an efficient online/offline ID-based signature scheme which does not require any certificate attached to the signature for verification, and does not require any pairing operation in both signature generation or verification. More importantly, the offline signing algorithm does not require any secret key information. It can be pre-computed by a PKG. The offline information can also be re-used. This is a great advantage in WSN environments as the offline information can be hard-coded to the sensor node in the manufacturing or setup stage. It can eliminate any communication between the sensor node and the base station for the offline signing, which is considered as a costly factor in the WSN. The length of this (pre-computed) offline information, or can be considered as public parameters, is about 160 group elements. It may be considered long for signing a few messages. However, if the sensor requires to sign a thousand, or even a million of messages, these 160 group elements are just negligible when compared to those messages. Thus our scheme is particular suitable for large scale network. [2] Wireless sensor networks (WSNs) have recently attracted a lot of interest in the research community due their wide range of applications. Due to distributed nature of these networks and their deployment in remote areas, these networks are vulnerable to numerous security threats that can adversely affect their proper functioning. This problem is more critical if the network is deployed for some mission-critical applications such as in a tactical battlefield. Random failure of nodes is also very likely in real-life deployment scenarios. Due to resource constraints in the sensor nodes, traditional security mechanisms with large overhead of computation and communication are infeasible in WSNs. Security in sensor networks is, therefore, a particularly challenging task. Author discusses the current state of the art in security mechanisms for WSNs. Various types of attacks are discussed and their countermeasures presented. A brief discussion on the future direction of research in WSN security is also included. In [3] author develop and analyze low-energy adaptive clustering hierarchy (LEACH), a protocol architecture for micro sensor networks that combines the ideas of energy-efficient cluster-based routing and media access together with application-specific data aggregation to achieve good performance in terms of system lifetime, latency, and application-perceived quality. LEACH includes a new, distributed cluster formation technique that enables self-organization of large numbers of nodes, algorithms for adapting clusters and rotating cluster head positions to evenly distribute the energy load among all the nodes, and techniques to enable distributed signal processing to save communication resources. In [4] author develop an M/G/1 model to analytically determine the delay incurred in handling various types of queries using our enhanced APTEEN (Adaptive Periodic Threshold-sensitive Energy Efficient sensor Network protocol) protocol which uses an enhanced TDMA schedule to efficiently incorporate query handling, with a queuing mechanism for heavy loads. It also provides the additional flexibility of querying the network through any node in the network. In [5] author proposed a security system for VANETs to achieve privacy desired by vehicles and traceability required by law enforcement authorities, in addition to satisfying fundamental security requirements including authentication, non repudiation, message integrity, and confidentiality. Moreover, we propose a privacy preserving defense technique for network authorities to handle misbehavior in VANET access, considering the challenge that privacy provides avenue for misbehavior. The proposed system employs an identity-based cryptosystem where certificates are not needed for authentication. [6] A new type of signature scheme is proposed. It consists of two phases. The first phase is performed off-line, before the message to be signed is even known. The second phase is performed on-line, once the message to be signed is known, and is supposed to be very fast. A method for constructing such on-line/off-line signature schemes is presented. The method uses one-time signature schemes, which are very fast, for the on-line signing. An ordinary signature scheme is used for the off-line stage.

III. PROPOSED ALGORITHM

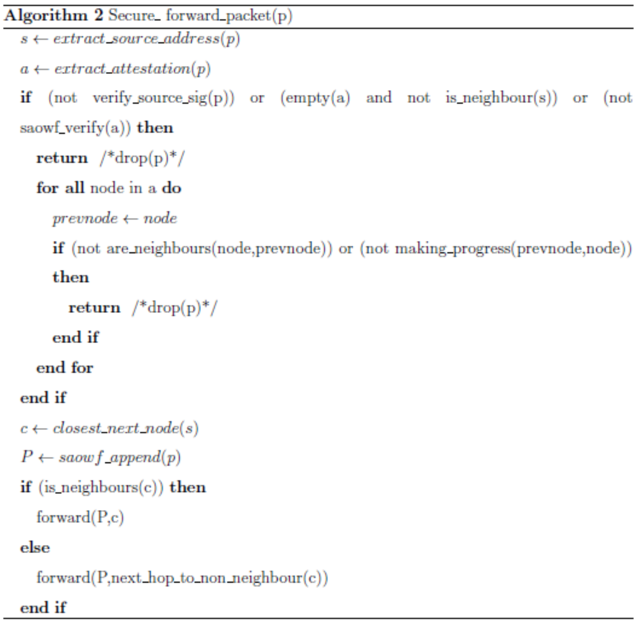
A. *Description of the Proposed Algorithm:*

The formal description : In PLGP, forwarding nodes do not know what path a packet took, allowing adversaries to divert packets to any part of the network, even if that area is logically further away from the destination than the malicious node. This makes PLGP vulnerable to Vampire attacks. So forwarding phase of PLGP is modified to avoid vampire attacks. No-backtracking property, is satisfied for a given packet if and only if it consistently makes progress toward its destination in the logical network address space. To preserve no-backtracking, we add a verifiable path history to every PLGP packet. The resulting protocol, PLGP with attestations (PLGPa) uses this packet history together with PLGPs tree routing structure so every node can securely verify progress, preventing any significant adversarial influence on the path taken by any packet which traverses at least one honest node. Whenever node n forwards packet p, it this by attaching a non replayable attestation (signature). These signatures form a chain attached to every packet, allowing any node receiving it to validate its path. Every forwarding node verifies the attestation chain to ensure that the packet has never travelled away from its destination in the logical address space. Following function Secure _forward _packet(p) defines the modified protocol.

IV. PSEUDO CODE



```
Algorithm 1 Forward_packet(p)
  $s \leftarrow extract\_source\_address(p)$
  $c \leftarrow closest\_next\_node(s)$
  if (is_neighbour(c)) then
    forward(p,c)
  else
    $r \leftarrow next\_hop\_to\_non\_neighbour(c)$
    forward(p,r)
  end if
```



```
Algorithm 2 Secure_ forward_packet(p)
  $s \leftarrow extract\_source\_address(p)$
  $a \leftarrow extract\_attestation(p)$
  if (not verify_source_sig(p)) or (empty(a) and not is_neighbour(s)) or (not
  saowf_verify(a)) then
    return /*drop(p)*/
    for all node in a do
      $prevnode \leftarrow node$
      if (not are_neighbours(node,prevnode)) or (not making_progress(prevnode,node))
      then
        return /*drop(p)*/
      end if
    end for
  end if
  $c \leftarrow closest\_next\_node(s)$
  $P \leftarrow saowf\_append(p)$
  if (is_neighbours(c)) then
    forward(P,c)
  else
    forward(P,next_hop_to_non_neighbour(c))
  end if
```

```
Algorithm 3 Modified_ discovery_ phase(node)
  if (transmit_power(node) > THRESHOLD ) then
    return /*drop(node)*/
  else
    insert_ into_ routingtable(node)
  end if
```

```
Algorithm 4 Modified_ forward_packet(p)
  s ← extract_source_address(p)
  a ← extract_attestation(p)
  if (not verify_source_sig(p)) or (empty(a) and not is_neighbour(s)) or (not saowf_verify(a)) then
    return /*drop(p)*/
    prevnode ← node
    if (not are_neighbours(node,prevnode)) or (not making_progress(prevnode,node)) then
      return /*drop(p)*/
    end if
  end if
  c ← closest_next_node(s)
  P ← saowf_append(p)
  if (is_neighbours(c)) then
    forward(P,c)
  else
    forward(P,next_hop_to_non_neighbour(c))
  end if
```

V. SIMULATION RESULTS

The simulation analysis for PLGP is implemented using Network Simulator NS2
The simulation is done for Energy consumption , Lifetime and Residual energy whose results are shown in Figure 1 ,2 & 3 respectively.

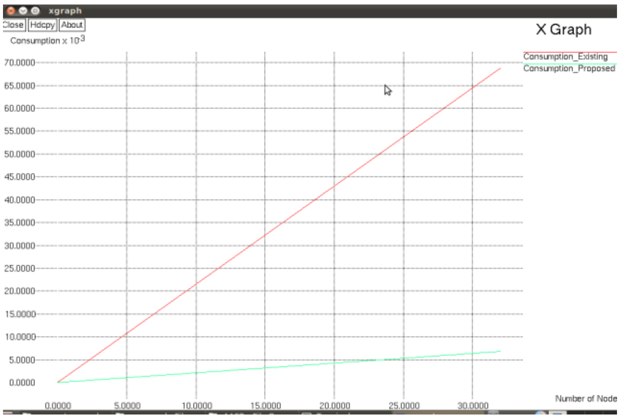


Figure 1 : Energy Consumption

The above figure shows that the Energy consumption of the proposed system is better than the existing system

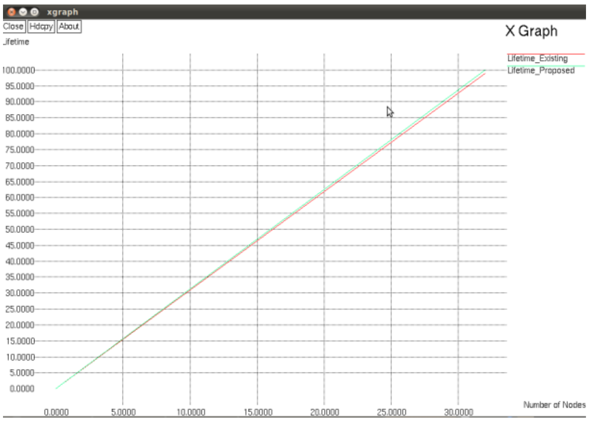


Figure 2 : Lifetime

The figure 2 shows that the lifetime of the proposed system is better than the existing system

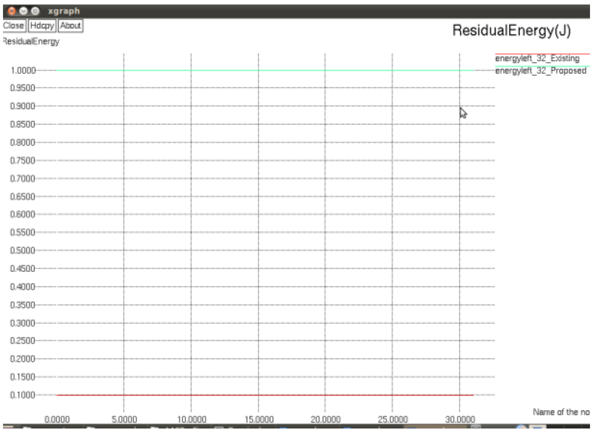


Figure 3 : Residual energy

The above figure shows that the residual energy of the proposed system is higher than the existing system

VI. Conclusion and Future Work

The Wireless Sensor Network is an emerging area which has wide applications. Hence the security in wireless sensor network is of great concern. Vampire attacks are important attack against a wireless sensor network in which an adversary develop and transmit messages that causes more energy to be consumed by the network than if an honest node transmitted a message of identical size to the same destination, although using different packet headers. So it is very important to detect the vampire nodes as early as possible. Here PLGP protocol is used to employ the vampire attacks. Since PLGP has two phases vampire node detection is also done in this two phases. The novel algorithm is the first sensor network routing protocol that provably bounds the damage from vampire attack in two phases of PLGP. This method reduces the energy utilisation, increases the lifetime. Here only PLGP protocol is considered, how the proposed solution works in other routing protocol is not considered. This method can be further extended to determine this problem.

References

1. J. Liu et al., “Efficient Online/Offline Identity-Based Signature for Wireless Sensor Network,” Int’l J. Information Security, vol. 9, no. 4, pp. 287-296, 2010.

2. Y. Wang, G. Attebury, and B. Ramamurthy, "A Survey of Security Issues in Wireless Sensor Networks," IEEE Comm. Surveys & Tutorials, vol. 8, no. 2, pp. 2-23, 2006
3. W. Heinzelman, A. Chandrakasan, and H. Balakrishnan, "An Application-Specific Protocol Architecture for Wireless Microsensor Networks," IEEE Trans. Wireless Comm., vol. 1, no. 4, pp. 660- 670, Oct. 2002.
4. A. Manjeshwar, Q.-A. Zeng, and D.P. Agrawal, "An Analytical Model for Information Retrieval in Wireless Sensor Networks Using Enhanced APTEEN Protocol," IEEE Trans. Parallel & Distributed Systems, vol. 13, no. 12, pp. 1290-1302, Dec. 2002.
5. J. Sun et al., "An Identity-Based Security System for User Privacy in Vehicular Ad Hoc Networks," IEEE Trans. Parallel & Distributed Systems, vol. 21, issue no. 9, pp. 1227-1239, Sept. 2010.
6. S. Even, O. Goldreich, and S. Micali, "On-Line/Off-Line Digital Signatures," Proc. Advances in Cryptology vol. 30, nos. 14/ 15, pp. 2826-2841, 2007.
7. A.A. Abbasi and M. Younis, "A Survey on Clustering Algorithms for Wireless Sensor Networks," Computer Comm., vol. 30, nos. 14/ 15, pp. 2826-2841, 2007.
8. Huang Lu, Student Member, IEEE, Jie Li, Senior Member, IEEE, and Mohsen Guizani, Fellow, Secure and Efficient Data Transmission for Cluster-Based Wireless Sensor Networks IEEE Transactions on parallel and distributed systems, Vol. 25, issue no . 3, March 2014
9. Eugene Y. Vasserman, Nicholas Hopper, " Vampire Attacks: Draining Life from Wireless Sensor Networks", IEEE transactions onmobile computing, Vol. 12, issue No. 2, February 2013.