INTERNATIONAL RESEARCH JOURNAL IN ADVANCED ENGINEERING AND TECHNOLOGY (IRJAET) E - ISSN: 2454-4752 P - ISSN : 2454-4744 VOL 5 ISSUE 2 (2019) PAGES 4270 - 4276
RECEIVED : 29.02.2019 PUBLISHED : 23.03.2019
March 23, 2019

SECURE DATA TRANSMISSION FOR CLUSTER BASED WIRELESS SENSOR NETWORKS

[1,2]GOWTHAM R, JAGADESH D,KAILASH V, Mrs.SUGANYA.K

[1,2]UG Scholar, Department of Computer Science and Engineering,

[3]Assistant Professor, Department of Computer Science and Engineering,

Kingston Engineering College. Kapadi, Vellore, Tamil Nadu

ABSTRACT

Understanding brilliant network digital assaults is key for creating suitable security and recuperation measures. Propelled assaults seek after amplified sway at limited expenses and perceptibility. This paper conducts hazard examination of joined information honesty and accessibility assaults against the power framework state estimation. We contrast the joined assaults and unadulterated trustworthiness assaults. A security file for weakness evaluation to these two sorts of assaults is proposed and detailed as a blended whole number straight programming issue. We demonstrate that such consolidated assaults can prevail with less assets assaults. The joined assaults with constrained learning of the framework show additionally uncover favorable circumstances in keeping stealth against the terrible information discovery. At long last, the danger of joined assaults to dependable framework task is assessed utilizing the outcomes from powerlessness evaluation and assault sway examination. The discoveries in this paper are approved and upheld by a nitty gritty contextual analysis. List Terms—Combined respectability and accessibility assault, chance investigation, control framework state estimation

1.INTRODUCTION

A class of data integrity attack, has been studied with a considerable amount of work .It has shown that with perfect knowledge of the system model and the capability to manipulate a certain number of measurements, the attacks can coordinate to keep stealth against the bad data detection. The analysis is supported with the results from the power system use case. The results shows how important the knowledge is to the attacker and measurements are more vulnerable to the attacks with limited resources.

2.EXISTING SYSTEM

- Existing LEACH-like protocols is challenging, because they dynamically, randomly and periodically rearrange the network's clusters and data links.
- There are providing steady long-lasting node-to-node trust relationships and common key distributions are inadequate for LEACH-like protocols (most existing solutions are provided for distributed WSNs, but not for CWSNs).
- This problem occurs when a node does not share a pair-wise key with others in its preloaded key ring, in order to mitigate the storage cost of symmetric keys, and the key ring is not sufficient for the node to share pair-wise symmetric keys with all of the nodes in a network.
- It cannot participate in any cluster, and therefore, has to elect itself as a CH.
- The orphan node problem reduces the possibility of a node joining a CH, when the number of alive nodes owning pair-wise keys decreases after a long term operation of the network.
- The orphan node problem increases the overhead of transmission and system energy consumption by raising the number of CHs.
- A sensor node does share a pair-wise key with a distant CH but not a nearby CH; it requires comparatively high energy to transmit data to the distant CH.

INTERNATIONAL RESEARCH JOURNAL IN ADVANCED ENGINEERING AND TECHNOLOGY (IRJAET) E - ISSN: 2454-4752 P - ISSN : 2454-4744 VOL 5 ISSUE 2 (2019) PAGES 4270 - 4276
RECEIVED : 29.02.2019 PUBLISHED : 23.03.2019
March 23, 2019

2.1DISADVANTAGES:

- Very high key Management storage, use symmetric algorithm.
- Lot of Cryptography problem occur in Cluster Based Wireless Sensor Network
- Require high Energy to transmit data to the CH.

3. PROPOSED SYSTEM:

- New approach applied and evaluated the key management of IBS to routing in CWSNs.
- In this project, to extend our previous work and focus on providing efficient secure data communication for CWSNs.
- Propose two Secure and Efficient data Transmission (SET) protocols for CWSNs, called SET-IBS and SETIBOOS, by using the IBS scheme and the IBOOS scheme, respectively.
- The key idea of both SET-IBS and SET-IBOOS is to authenticate the encrypted sensed data, by applying digital signatures to message packets.
- The proposed protocols, secret keys and pairing parameters are distributed and preloaded in all sensor nodes by the BS initially, which overcomes the key escrow problem described in ID-based crypto-systems.
- Secure communication in SET-IBS relies on the ID-based cryptography, in which, user public keys are their ID information.
- SET-IBOOS is proposed in order to further reduce the computational overhead for security using the IBOOS scheme, in which security relies on the hardness of the discrete logarithmic problem.
- The proposed protocols with respect to the security requirements and analysis against three attack models.
- Compare the proposed protocols with the existing secure protocols for efficiency by calculations respectively, with respect to both computation and communication.

3.1 ADVANTAGES:

- Efficient in data transmission
- Efficient for applying the key management for security.
- Effective communication and saves energy
- Solve the orphan node problem.
- Secured data transmission with a symmetric key management.

4.LITERATURE SURVEY

1.An Intrusion Detection System In Mobile Networks

Author: A. Gianni, S. Sastry, K. H. Johansson,2009

The nature of mobility for mobile networks needs additional mechanisms for providing security. These vulnerabilities do not exist in a fixed wired network. Therefore, the traditional way of protecting networks with firewalls and encryption software is no longer sufficient. We need to develop new architecture and mechanisms to protect the wire-less networks and mobile computing applications. Hence, in this paper, we discuss how to identify the intrusion after an anomaly is reported. Simple rules are applied to identify the intruder information and detect the type of the attack. A node called the Monitor node carries the identification process. This node overhears the channel and detects the misbehavior nodes.

There may be more than one monitor node in the whole network. Periodically the monitor nodes are elected in the network.

Disadvantages:

- First, a small window will result in false positives while a large window will result in irrelevant data as well as increase the chance of false negatives.
- Second, the net topology is only determined after considerable trial and error.
- The intruder can train the net during its learning phase**.**

2.A Novel Energy Efficient Routing Algorithm for Hierarchially Clustered Wireless Sensor Networks

Author: R. S. Ross,2012

Continued advances of MEMS and wireless communication technologies have enabled the deployment of large scale wireless sensor networks (WSNs) .The potential applications of WSNs are highly varied, such as environmental monitoring, target tracking and military surveillance. Sensors in such a network are equipped with sensing, data processing, and radio transmission units, while the power is highly limited. Due to the sensors' limited power, innovative techniques that improve energy efficiency to prolong the network lifetime are highly required. Thus energy-aware design has been a hot research area at all layers of the networking protocol stack. Data gathering is a common but critical operation in many applications of WSNs, where data aggregation and hierarchical routing mechanism are commonly used techniques. Data aggregation can eliminate data redundancy and reduce communication load. Hierarchical (clustering) mechanisms are especially effective in increasing network scalability and reducing data latency, and have been extensively exploited. We propose and evaluate an energy efficient clustering scheme (EECS) for periodical data gathering applications in WSNs. In the *cluster head election* phase, the cluster head is elected by localized competition, which is unlike LEACH, and with no iteration, which differs from HEED. The optimal value of competition range produces a good distribution of cluster heads. Further in the *cluster formation* phase, plain nodes join clusters not only taking into account its intra-cluster communication cost, but also considering cluster heads' cost of communication to the BS.EECS is autonomous and more energy efficient, and simulation results show that it prolongs the network lifetime much more significantly than the other clustering protocols.

Disadvantages:

- Unbalanced energy depletion.
- Performance of data transmission is too low.
- Here several cluster head is elected which is lead to damage system.

3.Efficient Algorithms for Pairing-Based Cryptosystems

Author: W. Wang and Z. Lu,2013

The recent discovery of groups where the Decision Diffie-Hellman (DDH) problem is easy while the Computational Diffie-Hellman (CDH) problem is hard, and the subsequent definition of a new class of problems variously called the Gap Diffie-Hellman, Bilinear Diffie-Hellman, or Tate-Diffie-Hellman [6] class, has given rise to the development of a new, ever expanding family of cryptosystems based on pairings, such as: Short signatures .Identity-based

encryption and escrow ElGamal encryption. Identity-based authenticated key agreement .Identity-based signature schemes. Tripartite Diffie-Hellman. Self-blindable credentials. The growing interest and active research in this branch of cryptography has led to new analyses of the associated security properties and to extensions to more general (e.g. hyperelliptic and superelliptic) algebraic curves .However, a central operation in these systems is computing a bilinear pairing (e.g. the Weil or the Tate pairing), which are computationally expensive. Moreover, it is often the case that curves over fields of characteristic 3 are used to achieve the best possible ratio between security level and space requirements for super singular curves, but such curves have received considerably less attention than their even or (large) prime characteristic counterparts. Our goal is to make such systems entirely practical and contribute to fill the theoretical gap in the study of the underlying family of curves, and to this end we propose several efficient algorithms for the arithmetic operations involved the definition of point tripling for super singular elliptic curves over F3m, that is, over fields of characteristic 3. A point tripling operation can be done in O (m) steps (or essentially for free in hardware); as opposed to conventional point doubling that takes O (m2) steps. Furthermore, a faster point addition algorithm is proposed for normal basis representation. These operations lead to a noticeably faster scalar multiplication algorithm in characteristic 3. An algorithm to compute square roots over Fpm in O(m2 log) steps, where m is odd and p _ 3 (mod 4) or p _ 5 (mod 8). The best previously known algorithms for square root extraction under these conditions take O (m3) steps. This operation is important for the point compression technique, whereby a curve point P = (x, y) is represented by its x coordinate and one bit of its y coordinate, and its usefulness transcends pairing-based cryptography. A deterministic variant of Miller's algorithm to compute the Tate pairing that avoids many irrelevant operations present in the conventional algorithm whenever one of the pairing's arguments is restricted to a base field (as opposed to having both in an extension field). Besides, in characteristics 2 and 3 both the underlying scalar multiplication and the final powering in the Tate pairing experience a complexity reduction from O(m3) to O(m2) steps. All of these improvements are very practical and result in surprisingly faster implementations.

Disadvantages:

- Slow reaction on restructuring and failures.
- Network latency and network traffic.
- Total energy consumed for packet delivery.

4.An Authentication Framework for Wireless Sensor Networks using Identity-Based Signatures: Implementation and Evaluation

Author: D. Deka, R. Baldick, and S. Vishwanath,2015

Authentication in Wireless Sensor Networks (WSNs) can be divided into three categories, namely base station to sensor nodes, sensor nodes to other sensor nodes, and outside users to sensor nodes. The problem of authenticated broadcast by the base station has been widely addressed We focus on the other two categories, namely the authenticated broadcast/multicast by the sensor nodes and the outside user authentication. To handle these two problems, we proposed an authentication framework for WSNs in using Identity(ID)- based Cryptography and Online/Offline Signature (OOS) schemes. This framework is comprised of two authentication schemes; quick authenticated broadcast/ multicast by sensor nodes and outside user authentication. The first scheme allows every sensor node in the network to broadcast or multicast authenticated messages very quickly without the involvement of the base station. All potential receivers can verify a message sent by any sender node in the network. It also allows sensor nodes on the path from the sender node to the receivers to verify a valid

message and drop false injected data. The second scheme enables all sensor nodes in the network to verify the legitimacy of any outside user without storing any user specific information. It allows a maximum possible number of legitimate users to access data from sensor nodes in a secure way. This scheme first authenticates a user and then establishes a session key for the secure exchange of user queries and sensor nodes data. The proposed framework uses an ID-based Online/Offline Signature (IBOOS) (an ID-based version of OOS) for the first scheme and an ID-based Signature (IBS) for the second scheme In Wireless Sensor Networks (WSNs), authentication is a crucial security requirement to avoid attacks against secure communication, and to mitigate against DoS attacks exploiting the limited resources of sensor nodes. Resource constraints of sensor nodes are hurdles in applying strong public key cryptographic based mechanisms in WSNs. To address the problem of authentication in WSNs, we propose an efficient and secure framework for authenticated broadcast/multicast by sensor nodes as well as for outside user authentication, which utilizes identity based cryptography and online/offline signature (OOS) schemes. The primary goals of this framework are to enable all sensor nodes in the network, firstly, to broadcast and/or multicast an authenticated message quickly; secondly, to verify the broadcast/multicast message sender and the message contents; and finally, to verify the legitimacy of an outside user.

This paper reports the implementation and experimental evaluation of the previously proposed authenticated broadcast/multicast by sensor nodes scheme using online/offline signature on Tinos and MICA2 sensor nodes.

Disadvantages:

- Scalability of network is low.
- Computation cost is high.
- Storage overhead is also high.

5.Vulnerability Assessment of AC State Estimation With Respect to False Data Injection Cyber-Attacks

Author: Gabriela Hug,2012

This paper introduces new analytical techniques for performing vulnerability analysis of state estimation when it is subject to a hidden false data injection cyber-attack on a power grid's SCADA system.

Specifically, we consider ac state estimation and describe how the physical properties of the system can be used as an advantage in protecting the power system from such an attack. We present an algorithm based on graph theory which allows determining how many and which measurement signals an attacker will attack in order to minimize his efforts in keeping the attack hidden from bad data detection.

This provides guidance on which measurements are vulnerable and need increased protection. Hence, this paper provides insights into the vulnerabilities but also the inherent strengths provided by ac state estimation and network topology features such as buses without power injections.

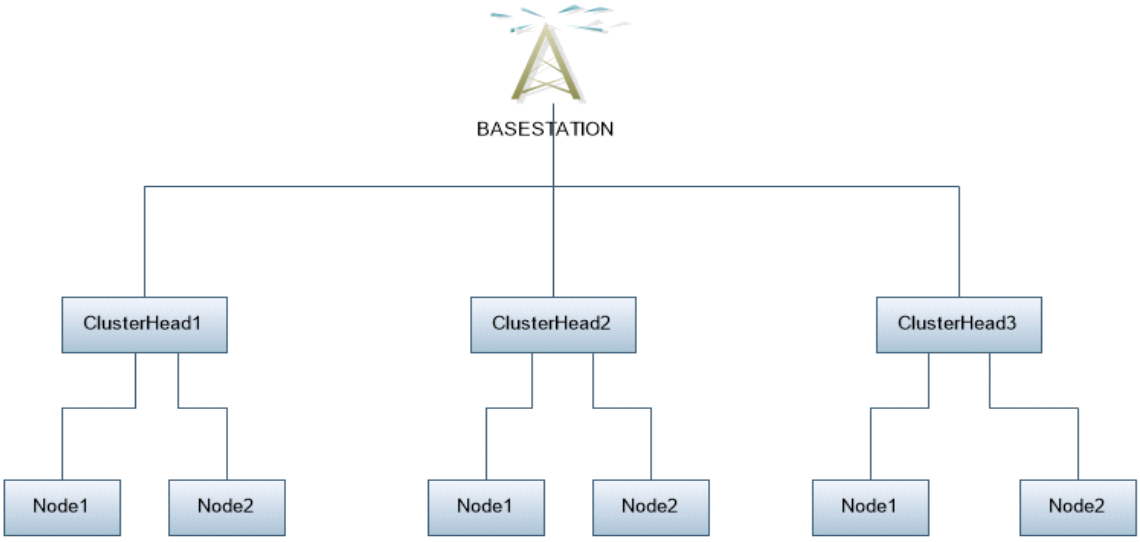
A deterministic variant of Miller's algorithm to compute the Tate pairing that avoids many irrelevant operations present in the conventional algorithm whenever one of the pairing's arguments is restricted to a base field (as opposed to having both in an extension field).

INTERNATIONAL RESEARCH JOURNAL IN ADVANCED ENGINEERING AND TECHNOLOGY (IRJAET) E - ISSN: 2454-4752 P - ISSN : 2454-4744 VOL 5 ISSUE 2 (2019) PAGES 4270 - 4276
RECEIVED : 29.02.2019 PUBLISHED : 23.03.2019
March 23, 2019

Disadvantage:

- It is subject to a hidden false data injection cyber-attack.
- The malicious intent might not be to hide the attack.
  Additionally,
    - Scalability of network is low.
    - Computation cost is high.
    - Storage overhead is also high.

5. SYSTEM ARCHITECTURE



6.CONCLUSION

In this paper, it is reviewed that he data transmission issues and the security issues in the cluster based wireless networks.

The deficiency of the symmetric key management for secure data transmission has been discussed.

In the evaluation section, we provided feasibility of the proposed SET-IBS and SET-IBOOS with respect to the security requirements and analysis against routing attacks.

It is then presented two secure and efficient data transmission protocols respectively for cluster based wireless networks, reliable data transmission identity based digital signature protocol.

In the evaluation section, it is provided feasibility of the proposed efficient data transmission identity based digital signature protocol with respect to the security requirements and analysis against routing attacks.

Data transmission identity based digital signature protocol is efficient in communication and applying the ID-based crypto-systems, which achieves security requirements in cluster based wireless networks, as well as solves the orphan node problem in the secure data transmission protocols with the symmetric key management.

7. FUTURE ENHANCEMENT:

From our project it is clear that by using the efficient algorithms like Risk Assessment Algorithm for decreasing the possibility of the occurrence of the attacks in the networks.And also the Shortest path algorithm called Dijkstra's algorithm is used for efficient path finding.

8. REFERENCES

1. T.Hara, V. I. Zadorozhny, and E. Buchmann, Wireless Sensor Network Technologies for the Info. Explosion Era, Stud. Comput. Intell. Springer-Verlag, 2010, vol. 278.
2. Y.Wang, G. Attebury, and B. Ramamurthy, "A Survey of Security Issues in Wireless Sensor Networks," IEEE Commun. Surveys Tuts., vol. 8, no. 2, 2006.
3. A.A. Abbasi and M. Younis, "A survey on clustering algorithms for wireless sensor networks," Comput. Commun., vol. 30, no. 14-15, 2007.
4. W.Heinzelman, A. Chandrakasan, and H. Balakrishnan, "An application-specific protocol architecture for wireless microsensor networks," IEEE Trans. Wireless Commun., vol. 1, no. 4, 2002.
5. 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 Distrib. Syst., vol. 13, 2002.
6. S.Yi, J. Heo, Y. Cho et al., "PEACH: Power-efficient and adaptive clustering hierarchy protocol for WSNs," Comput. Commun., vol. 30, no. 14-15, 2007.
7. K.Pradeepa, W. R. Anne, and S. Duraisamy, "Design and Implementation Issues of Clustering in Wireless Sensor Networks," Int. J. Comput. Applications, vol. 47, no. 11, 2012.
8. L B. Oliveira, A. Ferreira, M. A. Vilac¸a et al., "SecLEACH-On the security of clustered sensor networks," Signal Process., vol. 87, 2007.
9. P Banerjee, D. Jacobson, and S. Lahiri, "Security and performance analysis of a secure clustering protocol for sensor networks," in Proc. IEEE NCA, 2007.
10. K.Zhang, C. Wang, and C. Wang, "A Secure Routing Protocol for Cluster-Based Wireless Sensor Networks Using Group Key Management," in Proc. WiCOM, 2008.