International Journal of Early Childhood Special Education (INT-JECSE)
DOI:10.9756/INTJECSE/V14I5.949 ISSN: 1308-5581 Vol 14, Issue 05 2022

A Novel Secured Data transmission and authentication technique in large WSNs

T V Krishna Chowdary[1], K.V.V. Satyanarayana[2]
[1]Research Scholar, Department of Computer Science and Engineering, Koneru Lakshmaiah Education Foundation
(KLEF), Green Fields, Vaddeswaram, Guntur Dist, Andhra Pradesh, INDIA.tkrishna09@gmail.com

[2]Professor, Department of Computer Science and Engineering, Koneru Lakshmaiah Education Foundation
(KLEF), Green Fields, Vaddeswaram, Guntur Dist, Andhra Pradesh, INDIA.

Abstract: With the exponential growth of network bandwidth and computational resources, data authentication and confidentiality have become one of the interesting research areas in wireless networks. Authentication is considered as a prime concern in the field of energy-constrained wireless sensor networks due to its wide domain applications. Wireless network networking is a recent model for the growing trend of broadband networking, which serves a wide variety of applications. The high-speed service delivery is available to end users, since wireless networks rely on the multi-hop wireless backbone for data supply without the need to use a fixed infrastructure.Using integrity, secured key distribution and encryption models, most traditional data transmission and authentication models also fail to authenticate node behaviour. Experimental results have shown that, compared to traditional wireless authentication models , the proposed model has high computing speed, overhead storage and secured key distribution. A new trustworthy node authentication and protection model for path planning was introduced in complex wireless networks to solve these problems. This proposed model has introduced TACO and Incorporate Verification techniques for wireless initialization and confidence likelihood calculations. In this model, an integrated security based ant colony optimization has been introduced. Experimental findings have shown that the proposed model provides high speeds and strong data security in comparison with conventional wireless authentication models.

Keywords—WSN,Security , node integrity,trust node

1.INTRODUCTION

During the area monitoring and infrastructure monitoring process, Wireless Sensor Networks (WSNs) are designed and implemented to transmit sensitive data. All security systems must follow the criteria of honesty, confidentiality and authenticity. The entire network is a series of very small, intelligent devices, also called sensor nodes. During the monitoring of various activities and environmental conditions, authentication and protection in wired networks are critical. Choosing and implementing a valid authentication protocol in this setting is difficult and complicated. Due to insufficient memory, power and resources, the issue arises. Since WSNs are used unattentively in the hostile environment, the risks of attacks are growing quickly. There is also a need for improved protection for WSNs[1]. The security monitoring mechanism can not be applied in WSN because of inadequate resources. A single sensor node needs a limited number of iterations to measure the trust of neighbouring nodes, and the major problem behind the consumption of maximum energy. Two adjacent sensor nodes are in some cases[2]. Communication inactive. In such instances, the confidence of neighbouring nodes can not be determined. Wireless Sensor Network (WSN) technologies are primarily used in situations in the real world where people can not contact people. It comprises a great number of sensor nodes that are randomly used. The battery normally drives these sensor nodes. These devices therefore have limited energy efficiency, machine and communication efficiency, limited memory and processing speed. Some network problems such as packet collisions and malicious attacks on the network level are more likely if the large number of sensor nodes in the communication channel remain inactive. This can contribute to the packet drop and the main explanation is that both network efficiency and throughput have been greatly reduced[3]. Defective nodes or faulty nodes are more vulnerable to various security threats. It increases the congestion problems by disseminating needless packets, overflowing with fake messages, interrupting or retransmitting the message several times. At the time of data contact the sensor nodes have a responsibility to track all neighbouring node behaviours[4] In addition, some problems with WMN protection in recent years have gradually increased with increased network use and new hardware[1]. Failure to maintain WMN protection, complex infrastructure in software and hardware, network monitoring, etc. WMN security aims primarily to ensure integral, confidential and usable Internet information. The protection of WMN thus relates not only to security strategies but also to the control and management of the network. Data safety is an important part of computer networks, involving technologies, protocols, instruments and techniques for blocking and securing malicious packets. The linked network is facing a new mission, that is "man in the center of the attack" and packet spoofing. The WMN Security Framework tracks and analyses network operations to assess when an attack occurs on approved networks. For harassment and irregular detection models, network logs are required as training material, whose quality will significantly impair the safety and prevention efficiency of WMN 's systems. The use of static intrusion detection tools and techniques[2] also makes it difficult to conclude that a specific activity of the network is anomalous or normal[3].

During the monitoring of various activities as well as environmental circumstances, route preparation, clone node prevention and protection in the WMN networks were of great importance [4]. Appropriate model of clones avoidance in the competitive WMN networks is a difficult and complex job. A single WMN node needs a small number of iterations to measure the confidence and the energy usage of the neighboring knots are the main problem. Two adjacent WMN nodes for contact are inactive in some situations. In such instances, the trust of neighboring nodes can not be determined. WMN network implementations are typically applied in real-world environments that can not reach individuals. It also comprises large numbers of WMN sensor nodes randomly deployed[5]. The battery normally powers these nodes. Therefore, the capacity, machine, and communication performance, limited memory and processing speed are limited to these devices. A 3D model, designed to plan autonomous helicopter routes, is employed in [9]. The model is hierarchically distinct and has an optimal solution at any hierarchical level using standard Dijkstra or A * graphic quest.

Autonomous WMN preparation consists of a process for making action decisions. To be successful, a planer needs to look inside and outside. It should be adaptive not only to the context in which the mesh node operates, but also to the changing state of the Mesh node. The single WMN route must be flyable and no known clone nodes must collide with the WMN. Known clone nodes are shown by means of a height map since maps from the geographical maps are readily accessible[6]. The clone node collection preferably contains a list of objects that can easily be distinguished by polygonal frontiers. All terrain data are however available in grid-level format, where incremental track controls are required. Ant Colony Optimization (ACO) was developed as a general objective optimization technique in the early 90's in the field of swarm intelligence [7]. ACO is a population dependent meta-heuristic that can solve a large number of problems in an approximate manner. A meta-heuristic frame is used to describe heuristic methods which can be applied with few changes to a variety of problems. Heuristics are designed to achieve computational efficiency or logical simplicity at the expense of precision or accuracy. The use of problem specific knowledge by heuristics[8] is commonly used to cultivate solutions.With the rapid advancement of the design of computer networks and communication technologies, it is difficult to locate the protection of WMN networks by conventional safety tools and techniques. All conventional cryptographic schemes are based on both mathematical methods and unproven machine constraints. The aforementioned category of algorithms is commonly used on hidden media-sharing applications. The main challenge is the issue of key distribution in traditional cryptographic algorithms. All cryptographer algorithms, which are symmetrical key cryptosystems and asymmetrical key cycles, are narrowly divided into two specific categories according to requirements. Both the encryption and decryption process involve the same key in the Symmetric Key Cryptosystem. But the Asymmetric Key Cryptosystem requires multiple keys, one for the encryption process and the other for the decryption process. Failure to maintain WMN protection, complex infrastructure in software and hardware, network monitoring, etc. The WMN protection framework collects and analyses network behaviour to decide whether an attack on approved networks occurs. Network log data as training data must be used both to harass and to identify suspicious detections, whose consistency largely affects the efficacy of the WMN protection and prevention systems[9].

Goyal, and so on. A new digital signature algorithm [10] was introduced using ACO-based elliptical curves and chaotic systems. They have incorporated one-way, 2D hyperchaotic mapping to develop their new approach using the public key algorithm. Their algorithm avoids double attacks on key signatures. The algorithm proposed can be applied in practice scenarios because it is secure , reliable and quick. Various works have been carefully reviewed in this section in the area of chaotic safe hash algorithms. Their priorities and empirical validations, the pros and cons of each strategy are evaluated and defined.

The low-cost wireless networks are commonly used in local area networks[11], large area networks and metropolitan area networks. DTWNs[12] are primarily responsible for addressing the problems of unreliable communication due to delay, losses, sporadic communications, and even the rapidly evolving direction from one node to the other. In these networks, it is easier to create ties between nodes with unreliable connectivity. It ensues that a packet is transmitted and stored at midnodes for a continuous network connectivity. Further, the existing network takes more time to authenticate when a node changes its location. In addition, these nodes can not be fully trusted. Therefore, very strong safety approaches are necessary for the development. The source node is required to encrypt data before data transmission. The encrypted data is transmitted and decrypted via the authenticated target node. An powerful and standard cryptosystem, such as:- Advanced Encryption Standard (AES) and DES can be introduced in such cases. Additionally, it is too difficult to incorporate new cryptography techniques for each node in the DTNs.

2.RELATED WORKS

A primary energy-efficient management WMN group was introduced by Chang, et.al[26]. This methodology is based on three different approaches to solving problems with protection and scalability. The results of this technology were analysed theoretically and showed that it was very scalable in nature in case of small wireless networking systems. Without rising overhead computation and connectivity, an energy-efficient safety cap is implemented.Wanget.al suggested one-way collision-resistant data hazing[18]. More work can be done in future to develop such algorithms such as MD4, MD5, SHA, etc. Different techniques were studied to measure storage trends on WMNs, leading to some storage and sharing problems. It also solves other problems including encryption, preservation of boundaries, and proof of data. All these activities are handled by the visual management system. Other advantages are: privacy of the individual, availability of data, secure sharing, etc. Each sensor has its own view and a safe border.

MD5-ACO and MAC methods have been combined to incorporate their imperative properties, which are known as the rolebased access control (RBAC), a newly developed method from the above integration. The DAC approach is the discretionary sensor approach while the MAC technology is focused on grids. The methodology for attributes-based coding is suggested in [13] in order to address the drawbacks of the RBac approach. Nearly every approach to access control is PKI based. The basic principle of public key-based encryption enables the sending application from the Key Distribution Center (KDC) to trigger both the encryption and the encryption process. The Public Key Infrastructure (PKI) signs and sends it to the requester to authenticate the public. The sender requires the public key to successfully execute the encryption operation. The encrypted message in the unsecure WMN channel is sent from sender to recipient. To decrypt the cypher text message that is previously encrypted by the sender, the recipient must use a private key.

The ACO-IBE process consists of four algorithmic steps, such as initialization, keygen, encryption and decryption. The configuration algorithm generates the receiver master key. The recipient must then check his identity using the unique identities of SSN; email to the PKG. The KeyGen identity algorithm generates the private key for the recipiente. The sender is aware of the recipient identity during encryption (email). The sender uses the identity of the recipient to effectively perform the encryption operation. In order to decrypt encrypted message, the receiver needs its own private key created by PKG. The main benefit of introducing IDB (IBE) technical WMNs, is that, since the sender is already aware of the identity of the recipient, it is not necessary to contact the Key Distribution Center (KDC) to produce a public key. The previously suggested method of encryption based on attributes addresses the problems of the IBE WMN approach. The core policy of Attribute Based Encryption (ABE) is correlated with the identity of the sensor, in accordance with the conventional ABE process. The general encryption process involves four main algorithms: Setup, KeyGen, Encryption and Decryption. The main ones to be used in this process are the following. While WMNs have a powerful and reliable server, there are various external and internal threats[14] which are vulnerable to WMN. There can also be compromise on the security of data, data integrity and data availability. In order to maintain their integrity, untrusted service providers often mask such weakness from their system. Often the storage space of WMNs is expanded when the less used data is removed [15]. Many sensors and businesses store sensitive data in WMNs[16].

If an attack occurs, the intruder will obtain all sensitive data relating to companies and sensors[20].

- Capable of choosing decryption of the WMN sensor data in cypher form, the main policy-based encryption attribute is.
- Encrypting key policy functions

3.PROPOSED MODEL

Chaotic Bernoulli-Logistic Encryption: In order to enhance the overall volatility and stationary of cryptograph, a novel chaotic hash based technique is developed. It is basically an integration of Bernoulli- Logistic with chaotic systems. Logistic mapping is a traditional chaotic mapping technique which results more complex behaviours from the intervals [0,1] into [0,1].

A. Setup Scheme:

Let G be the bilinear group with prime order p
and generator k ,which statisfies bilinear property
and non-degeneracy property such that $\theta_1, \theta_2 \in G_p$.
The public key and master key can be generated as

$$\mathrm{PublicKey(Pk)} = \{\mathrm{ChaoticHash(Sharedkey)}, G_p, k, m = k^{\theta_2}, n = k^{1/\theta_2}, e(k,k)^{\theta_1}\}$$

$$\mathrm{MasterKey(Mk)} = \{\theta_2, k^{\theta_1}\}$$

B. Encrypt Scheme: The encryption algorithm takes the original plain text message (M) as input and generates the desired cipher text. The encryption technique encrypts the message M using the access tree structure T. Starting with the root node , this technique selects a random number r in p–integer modulo Z and sets q(R,0)=r. For the intermediate nodes x, it sets q(x,0)=q(parentnode(x,index)). Let L be the set of leaf nodes in access tree structure, then the cipher text is generated based on the given access tree structure T as:

$$\mathrm{CipherText(C)} = \{C^1 = M.e(k,k)^{\theta_1 . r}, T, C^2 = m^r,$$

$$\text{forall } x \in X: C_x = k^{q(x,0)}, C^1_x = H(A(x))^{q(x,0)}$$

C. KeyGen Scheme: The KeyGen algorithm generates private key (PrK) using the attributes' set (A). The KeyGen algorithm takes set of attributes A, sharedkey as input and generate secret key as output. This algorithm selects a random number r and rand$_j$ for each attribute A$_j$ and these random numbers are selected as the factor of sharedkey and holds in Z$_p$.

$$\mathrm{SecretKey(Sk)} = \{D' = k^{(\theta_1 + rand)/\theta_2}, D(j) = k^{rand*H(j).rand_j}, D'(j) = k^{rand_j}\}$$

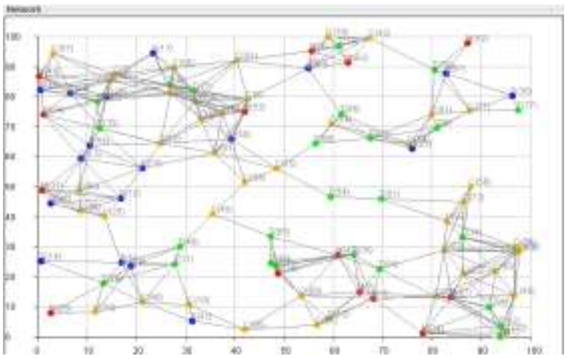
D. Decrypt Scheme: It accepts private key (Sk, attributes' set (A)), cipher-text (C, embedded with the access structure (T)),and public key (PK) as input. Decryption process is executed recursively. A recursive procedure is executed with three parameters cipher text, secret key , attributes set A and the node x from access tree.

Node2Node Data security:

In this approach, node to node data security is provided using three phase encryption model. This framework is based on the open source CP-ABE framework with customised key generation process. In this approach, each user's integrity value is used as key for the policy construction process.

4.EXPERIMENTAL RESULTS

Using the java-based WSNs simulator it was implemented. Experimental results show that because of its limited use of bandwidth, delay , packet drop and overhead this device is very efficient. It also strengthens the conventional security process, strengthens distribution and improves throughput. The proposed trust likelihood measurement is quicker in terms of performance and runtime than the conventional trust computing steps. The runtime of confidence measurement was increased to 20 to 30 percent for broad WSNs. In addition to trust calculations, the runtime with the variable hash size of the integrity check of each node was optimised. The results of the experiments are compared to conventional faith, honesty and encryption models.



.

Figure 3: Initialization of dynamic WSNs with 200 nodes.

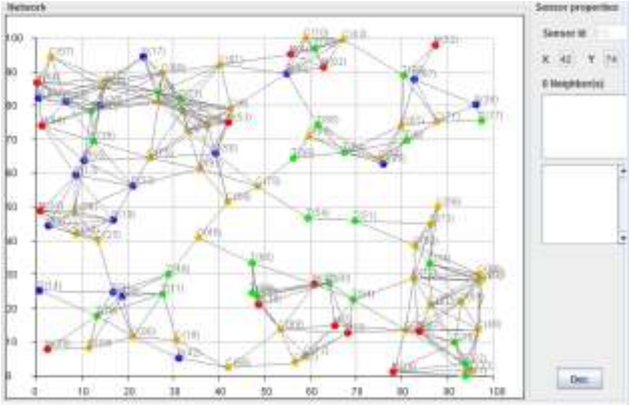


Figure 6: Above screenshot shows the Malicious node 53 and its empty neighbour nodes.

In the figure 6, neighbour nodes are empty due to the failure of integrity verification process.

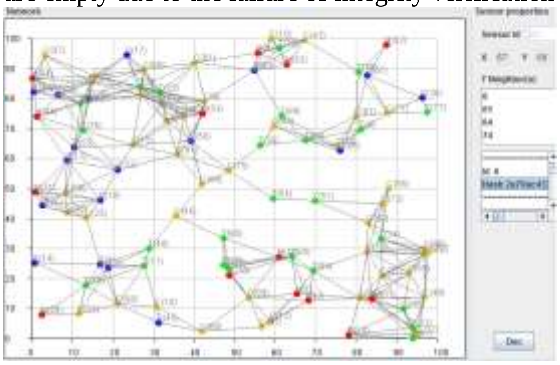


Figure 6: Above screenshot shows the trusted node 63 and its trusted neighbour nodes.

In the figure 6, neighbour list of the trusted node with node id, hash value and its encrypted data are shown in the corresponding list box.

Table 1: Comparison of proposed integrity model to existing integrity models

WSN's Nodes	MD5 WSNs (ms)	SHA512 WSN (ms)	HMAC WSN (ms)	logistic Chaotic WSN(ms)	Proposed Integrity Model(ms)
50	8373	8204	7934	7241	6613
100	16834	15799	15293	14973	13153
150	25934	25183	24183	23934	23735
200	36389	35692	32843	31936	29103
250	46116	43962	43108	42739	40242

Table 2:Comparison of encryption and decryption runtime for proposed model to the existing models

Average Runtime(ms)		
Model	EncryptionTime	DecryptionTime
AES	4972	3974

ECC	4846	3586
ABE	4146	3285
KPABE	3967	3163
Proposed	2894	2719

Table 3: Comparison of energy and packet delivery ratio of the proposed model to the existing models

Avg. Number of Sensor Node=200		
Model	**Accuracy**	**Energy(%)**
ACO+WSN	95.67	57.76
TACO+WSN	97.14	49.79
MOACO+WSN	98.05	43.13
ProposedModel	99.04	37.45

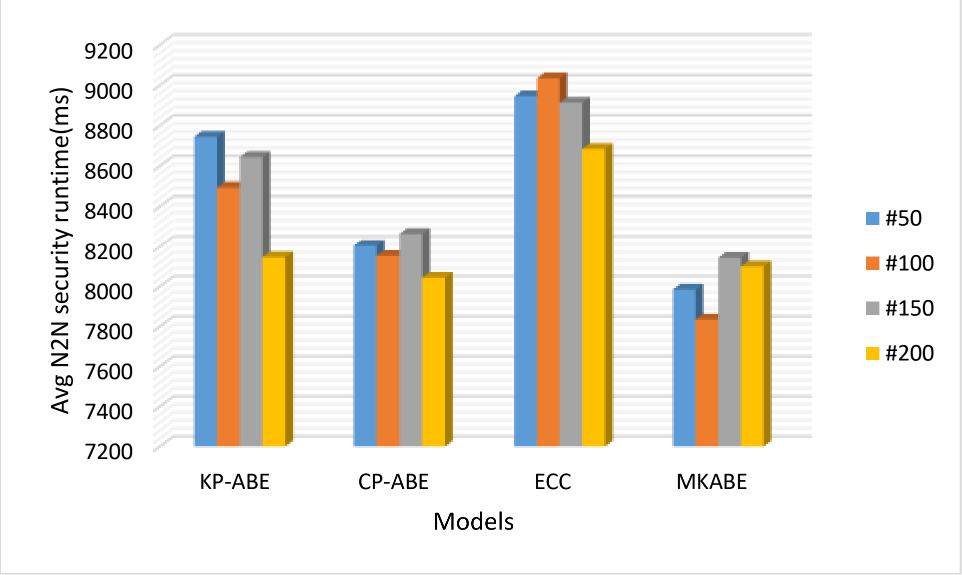


Figure 7: Comparative analysis of different security approaches on N2N security checking.

5.CONCLUSION

WSNs are typically used in insecure environments in which attacker can exploit those nodes through theft of credentials, reprogramming, etc. This paper has built and established a new data protection architecture for large WSNs to optimize the performance of diverse wireless sensor networks with confidence, security and authentication. Some schemes for the detection of clone node attacks are proposed, but nothing is being done to avoid this assault on major WSNs. For example , data poisoning attacks and confidentiality breaches of aggregate data are such risks. In this example, the proposed algorithm for data transmission and security authentication is used to construct a dynamic network topology initially. In this case, the trust likelihood value is used to configure all wireless nodes dynamically. In the next step, malicious nodes are removed through a verification method of probability and integrity. Each node is verified using the proposed integrity verification feature after the inception of the ACO-based network topology. To detect the malicious clone node, each node is checked against its integrity. In addition, the ciphertext policy attribute dependent encryption techniques for malicious attacks encrypt each sensor node data. Experimental results demonstrated that the integrated solution proposed is safer, more effective and more efficient in terms of resources, time and throughput than conventional confidence-based models.

References

1. W T Wang K F Ssu W C. Chang "Defending Sybil attacks based on neighboring relations in wireless mesh networks [J]" Security &amp; Communication Networks vol. 3 no. 5 pp. 408-420 2010.
2. Y. Yang W. Zhang Y. Hu "Research on algorithm of joint location based on ultra wideband" J. Northeast DianliUniv.. vol. 35 no. 1 pp. 83-87 2015. .
3. J. Li X. Zhong C. Xu "Review of dynamic node localization algorithm for wireless mesh networks" J. Northeast Dianli Univ. vol. 35 no. 01 pp. 52-58 2015.
4. B. Wu J. Chen J. Wu M. Cardei "A survey of attacks and countermeasures in Wireless Mesh Networks" Wireless Network Security Springer pp. 103-135 2007.

5. C.X. Liu T.L. Huang "Research on improved DV-hop algorithm against wormhole attacks in WSN" J. Sens. Technol. vol. 24 no. 10 pp. 1473-1478 2011.
6. J. Britos, "Statistical Intrusion Detection in Data Networks", IEEE Latin America Transactions, vol. 5, no. 5, 2007, pp. 373-380.
7. M. Mizutani, K. Takeda and J. Murai, "Behavior rule based intrusion detection", Proceedings of the 5th international student workshop on Emerging networking experiments and technologies - Co- Next Student Workshop '09, 2009, pp. 1254-1263.
8. S. Lu L. Li K. Lam L. Jia "SAODV: A WMN routing protocol that can withstand black hole attack" Computational Intelligence and Security 2009. CIS'09. International Conference On pp. 421-425 2009.
9. Elhadi M. Shakshuk Nan Kang Tarek R. Sheltami "EAACK - A Secure Intrusion Detection System for WMNs" IEEE Transactions On Industrial Electronics vol. 60 no. 3 March 2013.
10. Yih-Chun Hu Adrian Perrig David B. Johnson "Ariadne: A secure on-demand routing protocol for ad-hoc networks" Wireless networks vol. 11.1–2 pp. 21-38 2005.
11. Chowdary, K., & Satyanarayana, K. V. V. (2017). Malicious node detection and reconstruction of network in sensor actor network. Journal of Theoretical and Applied Information Technology, 95(3), 582-591
12. Kiranbabu, M. N. V., & Satyanarayana, K. V. V. (2017). Acquiring possible cost to client usage of CSP resources imposing knapsack approach on SLA's negotiations requirements. Journal of Advanced Research in Dynamical and Control Systems, 9(Special Issue 12), 1822-1832.
13. Krishna Chowdary, T. V., & Satyanarayana, K. V. V. (2017). A novel secured data transmission and authentication technique against malicious attacks in WSNs. Journal of Advanced Research in Dynamical and Control Systems, 9(Special Issue 18), 161-173.
14. Gupta, P., Satyanarayan, K. V. V., & Shah, D. D. (2018). IoT multitasking: Development of hybrid execution service oriented architecture (HESOA) to reduce response time for iot application. Journal of Theoretical and Applied Information Technology, 96(5), 1398-1407.
15. kiran, K. T. P. S., Satyanarayana, K. V. V., & Yellamma, P. (2018). Advanced Q-MAC: Optimal resource allocating for dynamic application in mobile cloud computing using QoS with cache memory. International Journal of Engineering and Technology(UAE), 7(3.1 Special Issue 1), 143-146.
16. Leela Sandhya Rani, Y., Sucharita, V., & Satyanarayana, K. V. V. (2018). Extensive analysis on generation and consensus mechanisms of clustering ensemble: A survey. International Journal of Electrical and Computer Engineering, 8(4), 2351-2357. doi:10.11591/ijece.v8i4.pp2351-2357