Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 4, Issue. 5, May 2015, pg.53 – 70

RESEARCH ARTICLE

A SURVEY ON AUTHENTICATION AND SECURITY MAINTENANCE IN WIRELESS SENSOR NETWORK

Ms.L.Devi., M.C.A.,M.Phil.,

Research Scholar (Ph.D)

Bharathiar University

Coimbatore

Dr.S.P.Shantharajah,M.C.A.,Ph.D.,

Professor, Department of MCA

Sona College of Technology

Salem-636005

ABSTRACT

Wireless sensor networks (WSN) are used to examine and to maintain the physical or environmental conditions like temperature, sound, pressure, etc. and utilized to pass the information through the network to a main location. The wireless networks are bi-directional that helps in controlling and maintaining the sensor activities. Wireless sensor networks are used in many security attacks with false data injection, data forgery, and overhearing. A large sensor network with the individual sensor nodes aims on security factor. A node injected into the sensor network for the data forwarding results in several attacks. These attacks are results in the injection of false data in the wireless sensor network. In a large scale wireless sensor network, detecting reports injected by compromised nodes is a large research confront. If a node is cooperated, all the security information collects the nodes are turns out to be accessible to the attacker. In order to increase the maintenance and security level in the wireless sensor networks, authentication system is designed. In this authentication system, the security maintenance level is

increased by filtering the false data. The wireless sensor networks aims on extracting the injected false data attack and the mitigation technique is designed for high security maintenance. The filtering false data are executed earlier to ease the system with the high security. Our research work aims to increase the security and maintenance level in the wireless network.

1. INTRODUCTION

Wireless Sensors Network (WSN) authentication is a growing technology resulting from progress of different fields for minimizing the false data attacks. In wireless sensor networks, sensor nodes introduce false data during both data aggregation and data forwarding. The false data detection technique takes false data injections during data forwarding and fails to permit alterations on the data by data aggregation. Many applications of wireless sensor networks (WSNs) depend on data about the positions of sensor nodes. The main aim of the routing protocols in sensor networks is the restricted ability of the nodes and the application of the exact nature of the networks to increase the security. Wireless sensor networks (WSNs) are used in unfocused environment where the energy replacement is a complex one. Because of the limited resources, a WSN needs to satisfy application specific QoS needs and to reduce the energy consumption to extend the system lifetime and security maintenance.

Wireless sensor networks (WSN) increased various research activity because of the exciting and convincing reasons offered by the potential for important monitoring applications on different subjects. The main aim of the sensor network is to separate tiny sensing devices that are capable of sensing alterations of incidents/parameters and corresponding with other devices over a particular geographic area for target tracking, surveillance, environmental monitoring etc. Security is employed from surrounding the characteristics of authentication, integrity, privacy, non-repudiation, and anti-playback.

Wireless Sensor Networks (WSNs) is network comprises of sensor nodes or motes communicating wirelessly with each other for improving the security level. Development in sensor, low power processor, and wireless communication technology aimed to the broad utilization of WSNs functions in modern world like broadcast authentication. Broadcast authentication is an essential and important security mechanism in a WSN because broadcast is a natural communication method in a wireless environment. When base stations need to send commands to thousands of sensor nodes, broadcasting is more efficient technique than unicasting to each node. Broadcast authentication is a

security service in wireless sensor networks (WSNs) that permits the mobile users of WSNs to broadcast messages to multiple sensor nodes in a secured way.

The authentication and security maintenance process in wireless sensor network aims to:

- To achieve high efficient bandwidth technique on reducing the gang injecting false data attack
- To enhance the authentication scheme on sensor network by overcoming the false data injection
- To maintain the system with high authentication scheme without any false data injection

This paper is organized as follows: Section II discusses authentication and security maintenance in wireless sensor network, Section III shows the study and analysis of the existing authentication and security maintenance techniques on wireless sensor networks, Section IV identifies the possible comparison between them and Section V concludes the paper, key areas of research is given as to improve the security level by filtering the false data.

2. ANALYSIS OF EXISTING LITERATURE

Wireless Sensor Networks (WSN) contains large number of resource limitations for sensor nodes in some applications. Bandwidth-efficient cooperative authentication (BECAN) scheme [1] filters the injected false data in wireless sensor network. BECAN accumulate energy by filtering the majority of inserted false data with minor extra overheads at the en-route nodes. But, BECAN fails to prevent/mitigate the gang injecting the false data attack from mobile compromised sensor nodes. The Data Aggregation and Authentication protocol (DAA) [2] combines false data detection. Identifies the false data inserted by a data aggregator for reducing the misusage of resources like bandwidth and battery power. Every sensor node can able to aggregate and forward data but fails to enhance the network security and efficiency.

Network Security architecture with ticket based protocol [4] assures the anonymous access control. It changes the hierarchical identity-based cryptography (HIBC) for inter domain authentication. Client's bandwidth allocation depending on the logged data is not effective in sensor network. Security Games for Node Localization using probabilistic approach [3] decides the repetition of the nodes. Game

theoretical situation for WSNs is verifiable multi-lateration is used however additional security counter calculates are taken place. Malicious node's max-min strategy resulting in the optimal strategy is not proved in wireless sensor network.

Virtual Energy-Based Encryption and Keying (VEBEK) scheme [5] is a secure communication framework where sense data is instructed using a permutation code created through the RC4 encryption mechanism. RC4 encryption alters function of the residual virtual energy of the sensor but threats on dynamic paths happened. Distributed Token Reuse Detection (DTRD) scheme for Privacy-Preserving Access Control for sensor network purchase the tokens from the network owner [6]. Efficient DTRD techniques for Distributed Privacy-Preserving Access Control scheme (DP2AC) under different attacker model are not studied. Virtual Ring Architecture as illustrated [9], it offers privacy protection in the smart grid environment with cost efficient factor. New security mechanisms are not maintained with future resource computing environments in wireless sensor network.

Multipath Routing for Intrusion Tolerance in Heterogeneous Wireless Sensor Networks [7] uses excellent design constraint settings at runtime due to environment alterations. Multipath route decision intrusions take place in sensor network system. Sequential mOnte carLo combIned with shadow-faDing estimation (SOLID) method follows the small scale primary data transferring. The main aim is to increase the temporal shadow fading correlation in sensing results induced by the primary user's mobility. Signal propagation was more random, the attack takes place in system with cruel adversaries on data forwarding.

3. AUTHENTICATION AND SECURITY MAINTANANCE IN WIRELESS NETWORKS

A Wireless Sensor Network (WSN) is a group of independent nodes communicating wirelessly over restricted areas with high authentication and increased level of security maintenance. Wireless Sensor Networks (WSNs) allowed the data gathering from a huge geographical region and designed chances for broad range of tracking and monitoring applications from both civilian and military domains. WSNs are supposed to process, store, and provide the sensed data to the network users on their demands.

3.1 Security Games for Node Localization through Verifiable Multilateration

Node localization is significant in wireless sensor network (WSN) applications. Location is employed to enhance the routing and saving power and to design applications where services are location reliant. A method is used to compute node reputation and the related accuracy of the monitored data is required. Definite approach is employed to limit nodes when few are cooperated and it is called as Verifiable Multilateration (VM). VM calculates an unknown position by leveraging on a set of trusted landmark nodes called as verifiers. VM can also able to identify reliable localization measures and definite cruel performances. Multilateration is the most important technique employed in WSNs to approximate the coordinates of unknown nodes specified by the positions of landmark nodes called as anchor nodes whose positions are identified. The position of unknown node is calculated by geometric inference based on the distances between the anchor nodes and the node. However, malicious node's maxmin strategy corresponds to the optimal strategy is not proved. It fails to extend the framework to handle multiple malicious nodes. Additional security counter measures are not carried out in this process.

3.2 Design and Performance Analysis of a Virtual Ring Architecture for Smart Grid Privacy

Virtual ring architecture is designed to ensure privacy protection of smart grid users. The virtual ring forms a network of smart meters belonging to the same geographical region. For planning purposes, the energy supplier fails to know the energy consumption of a particular smart meter than the total energy consumption of a particular geographical region. The smart meters of the same virtual ring share the related pair of keys that contains a public key and a private key. The virtual ring's key pair is the pair of keys created by the energy supplier and increased on every smart meter of a particular virtual ring. In place of containing a set of neighbors, every smart meter in a particular virtual ring has only two neighbors – a clockwise one (upstream neighbor) and an anticlockwise one (downstream neighbor).

Each smart meter in the ring take cares the receiving data from its downstream neighbor and sending data to its upstream neighbor. The upstream/downstream neighbors of a particular smart meter are not needed for the closest two neighbors to the specific smart meter. Each smart meter contains a

copy of the energy supplier certificate. The energy supplier connects to any smart meter to modernize the upstream/downstream neighbors of a particular smart meter. Each virtual ring contains an identifier (IDVR*)*. However, new security mechanisms Is not supported with future resource computing environments.

3.3 Integration of False Data Detection with Data Aggregation and Confidential Transmission in Wireless Sensor Networks

Wireless sensor networks are exposed to security attacks with false data injection, data forgery, and eavesdropping. Sensor nodes cooperated by intruders, and the compromised nodes alter data integrity by inserting the false data. The transmission of false data reduces the restricted battery power and alters the bandwidth usage. False data are injected by compromised sensor nodes in many ways with data aggregation and relaying. As data aggregation is significant to minimize data redundancy and/or to enhance the data accuracy, false data detection is significant to the condition of data integrity and efficient usage of battery power and bandwidth. Data confidentiality chooses data to be encrypted at the source node and decrypted at the destination. But, key establishment process is more vulnerable to node compromise attacks. False data detection and data confidentiality increase the communication overhead. Every sensor node is capable of both aggregating and forwarding data but does not improve network security and efficiency.

3.4 SAT: A Security Architecture Achieving Anonymity and Traceability in Wireless Mesh Networks

The wireless mesh backbone consists of mesh routers (MRs) and gateways (GWs) linked by common wireless links. Mesh routers and gateways serve as the access points of the WMN. The hospital, campus, enterprise, and residential buildings are examples of individual WMN domains promising to the Internet services from upstream service providers.

Each WMN domain, or trust domain is controlled by a domain administrator which serves as a trusted authority (TA), the central server of a campus WMN. The TA and associated gateways are linked by high-speed wired or wireless links. TAs and gateways can manage complex tasks. Besides, they are kept in private places and fails to compromise because of their significant roles in the WMN. In the WMNs of interest, TA offers free Internet access however needs the clients (CLs) to be approved and

associated members for a long term. In order to continue security of the network beside attacks and the fairness among clients, the home TA control the access of each client by concerning tickets depending on the misconduct of the client that reflects the TA's confidence about the client to perform. Ticket issuance happens when the client attempts to work with the network. After attaining a valid ticket, the client deposit it anytime the network service is preferred before the ticket terminates using the ticket deposit protocol. Next, in fraud detection, fraud is used interchangeably with misbehavior, that is basically an insider attack. Ticket reuse usually results from the client's inability to attain tickets from the TA when network access is desired, because of the client's past misbehavior that results the TA to constrain his ticket requests. After the fraud detection, ticket revocation is needed when a client is compromised and so entire secrets are revealed to the adversary.

3.5 VEBEK: Virtual Energy-Based Encryption and Keying for Wireless Sensor Networks

The VEBEK framework contains three modules:

- Virtual Energy-Based Keying
- Crypto, and
- Forwarding

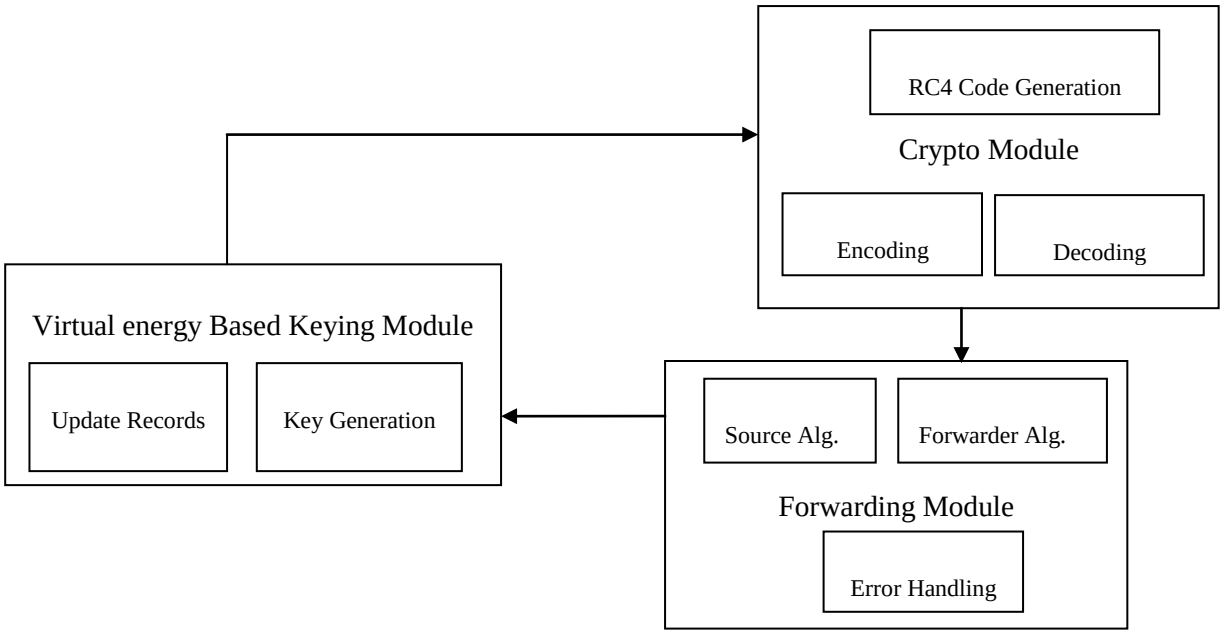

Fig.1 Structure of VEBEK Framework

The virtual energy-based keying process engages the formation of dynamic keys. In contradiction to dynamic keying schemes, it fails to exchange additional messages to establish keys. A sensor node computes keys based on its residual virtual energy of the sensor. The key is supplied to the crypto module. The crypto module in VEBEK uses a simple encoding process for the process of permutation of the bits in the packet consistent with the dynamically created permutation code created through RC4. The encoding is a simple encryption mechanism adopted for VEBEK. VEBEK's flexible architecture permits for approval of encryption mechanisms in lieu of encoding. Forwarding module controls the technique of sending or receiving of instructed packets beside the path to the sink. The virtual energy-based keying module of the VEBEK framework is significant technique employed for controlling the keying process. In VEBEK, each sensor node includes virtual energy value in the network. The rationale for employing virtual energy resisted to real battery levels.

The VEBEK protocol gives three security services: Authentication, integrity, and non-repudiation. The main aim of the services is the watching mechanism. The watching mechanism requires nodes to store one or more records to compute the dynamic keys employed by the source sensor nodes to decode packets and to catch invalid packets because of communication issues or potential attacks. The VEBEK framework requires for flexibility and maintains two operational modes: VEBEK-I and VEBEK-II. The operational mode of VEBEK decides the number of nodes a particular sensor node.

3.6 Distributed Privacy-Preserving Access Control in Sensor Networks

DP2AC called Distributed Privacy-Preserving Access Control scheme is planned for single-owner multiuser sensor networks. In DP2AC, all users engaged in sensed data acquires tokens from the network owner before penetrating the sensor network after sending a query with an unspent token to sensor node. After authenticating the token, the sensor node offers the user with suitable amount of requested data matching with the quantity of the token. Token generation involves blind signature results in a desirable property: the validity of each token verified by any sensor node, but the identity of the token holder is not known. The network owner avoids illegal access to sensed data while users defend their data access privacy. Each token in DP2AC is a random bit string with no connection to user identities. The key for token-reuse detection (TRD) is to allow each sensor node ensure with an in network base station where the token was not spent and decline the data access request.

In DTRD schemes, each node records all token that receives from its buffer. Accepting the Bloom filter decrease the storage cost of DTRD schemes or facilitate sensor node to accumulate an indefinite number of tokens at increasing false positives. The storage cost for each scheme is a constant that fails to change with the number of tokens stored.

3.7 Redundancy Management of Multipath Routing for Intrusion Tolerance in Heterogeneous Wireless Sensor Networks

Redundancy management of heterogeneous wireless sensor networks (HWSNs) using the multipath routing to respond user queries in the existence of unreliable and malicious nodes. The tradeoff issue becomes more difficult when inside attackers are exist as a path is broken when a malicious node is on path. It is in heterogeneous WSN (HWSN) environments where CH nodes contains more significant role in gathering and routing sensing data. HWSN contains sensors of various capabilities. Two types of sensors: CHs and SNs are taken. CHs are superior to SNs in energy and computational resources. CHs and SNs are allocated in the operational area. To guarantee the coverage, CHs and SNs are arranged randomly and distributed based on homogeneous spatial Poisson processes with intensities.

3.8 Robust Tracking of Small-Scale Mobile Primary User in Cognitive Radio Networks

Cognitive Radio (CR) helps to improve the spectrum efficiency by permitting secondary (unlicensed) users/devices to use spectrum opportunities that are temporarily unused by primary users (PUs). CRs are key components of efficient detection and reuse of spectrum opportunities so mitigating the spectrum-scarcity issues because of the unstable growth of wireless/mobile users, services and application. In CRNs, sensors are frequently used in hostile and unattended areas to capture by attackers. The compromised sensors reports controlled to increase localization error leads to the inefficient utilization of accessible spectrum or additional interference to PUs.

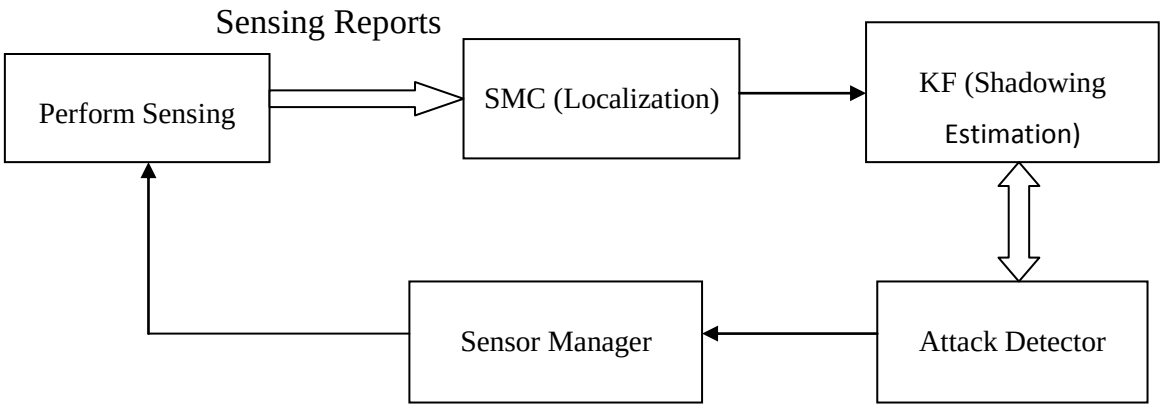

Fig. 2 SOLID Framework

RSS-based tracking scheme called SOLID enhances the conventional Sequential Monte Carlo (SMC)-based localization with shadow fading estimation. The shadowing estimation in SOLID develops localization performance. By monitoring temporally-correlated shadow fading, SOLID exactly identifies both manipulated and erroneous sensing reports, so attaining high robustness. The main aim is utilization of temporal shadowing association in attack identification of malicious sensors fails to control the physical-layer signal-propagation characteristics.

4. COMPARISON OF AUTHENTICATION AND SECURITY MAINTANANCE IN WIRELESS NETWORKS & SUGGESTIONS

In order to compare the authentication and security maintenance in wireless networks, number of users is taken to execute the experiment. The first performance metric is processing time, which is defined as the amount of time required to verify and maintain the security level of the user data. The second performance is false positive rate, which is defined as amount of malicious users detected while authenticating the user's details. The third performance is security level which is defined as level of privacy given to the user's data from other user. The fourth performance is the energy consumption which is defined as the amount of energy consumed while authenticating and maintaining the security of the user's data.

4.1 PROCESSING TIME

No. of Users (Number)	Processing Time (ms)		
	DAA protocol	Virtual Ring Architecture	NSA with ticket based Protocol
10	52	60	45
20	58	64	49
30	61	69	53
40	65	73	58
50	69	76	63
60	73	79	69
70	77	82	73

Table 4.1 Tabulation for Processing Time on Authentication and Security Maintenance in WSN

The processing time comparison takes place on existing Data Aggregation and Authentication (DAA) protocol, Virtual Ring Architecture, and NSA with ticket based Protocol.

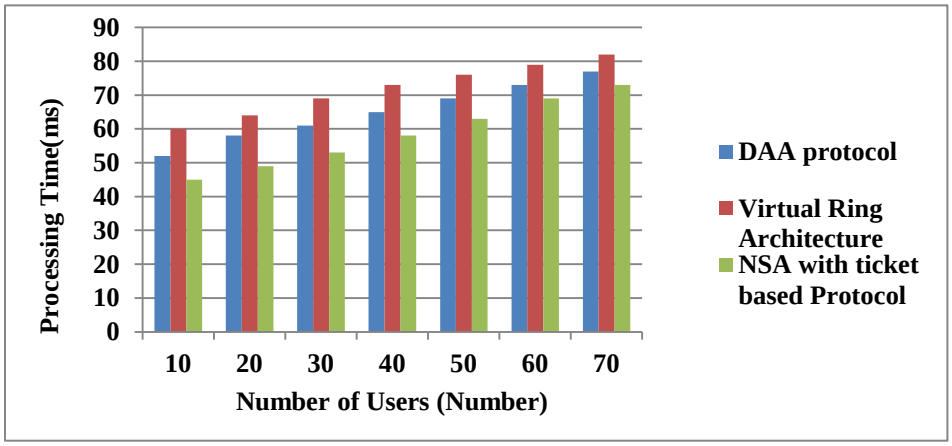

Fig. 4.1 Processing Time on Authentication and Security Maintenance in WSN

Fig 4.1 explains the processing time depending on the various authentication and security maintenance techniques. The processing time is measured in terms of milliseconds (ms). As the number of user's increases, processing time also increases automatically. The experiment shows that NSA with ticket based Protocol decreases the processing time when compared with Data Aggregation and Authentication (DAA) protocol and Virtual Ring Architecture. Research in NSA with ticket based Protocol is 5 – 16 % lesser processing time when compared with the Data Aggregation and Authentication (DAA) protocol and 10-15 % lesser processing time when compared with the Virtual Ring Architecture.

4.2 FALSE POSITIVE RATE

False positive rate is defined as amount of malicious users detected while authenticating and maintaining the security of the user's details. It is measured in terms of (%).

Number of Users(Number)	False Positive Rate (%)		
	VEBEK Scheme	MTTF Probabilistic System	Probabilistic Approach
10	52	69	81
20	48	65	76
30	44	56	70
40	42	52	64
50	40	49	58
60	39	45	52
70	36	43	48

Table 4.2 Tabulation for False Positive Rate on Authentication and Security Maintenance in WSN

The False Positive Rate comparison takes place on existing Virtual Energy-Based Encryption and Keying (VEBEK) scheme, Mean Time To Failure (MTTF) Probabilistic System, and Probabilistic Approach.

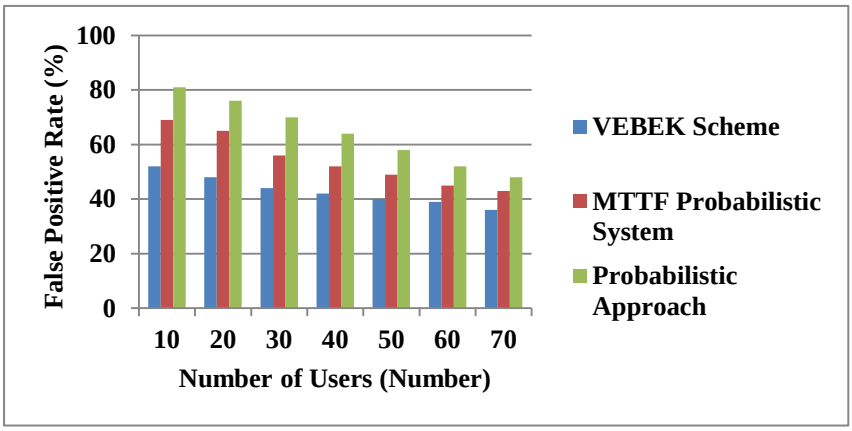

Fig. 4.2 False Positive Rate on Authentication and Security Maintenance in WSN

From fig. 4.2, false positive rate of existing systems on authentication and security maintenance techniques are described. False positive rate of Probabilistic Approach is comparatively higher than that of Virtual Energy-Based Encryption and Keying (VEBEK) scheme and Mean Time To Failure (MTTF) Probabilistic System. Research in the false positive rate of Probabilistic approach is 25-35% higher than

that of Virtual Energy-Based Encryption and Keying (VEBEK) scheme and 9-15%higher than that of Mean Time To Failure (MTTF) Probabilistic System.

4.3 SECURITY LEVEL

Security level is defined as the level at which the user data is kept at private level without allowing other user to access the data. It is measured in terms of percentage (%).

Number of Users (Number)	Security Level (%)	
	SOLID Method	DTRD Scheme
10	65	79
20	63	75
30	60	70
40	58	67
50	55	62
60	51	58
70	48	54

Table 4.3 Tabulation for Security Level on Authentication and Security Maintenance in WSN

The Security Level comparison takes place on existing Distributed token reuse detection (DTRD) Scheme, and Sequential mOnte carLo combIned with shadow-faDing estimation (SOLID) method.

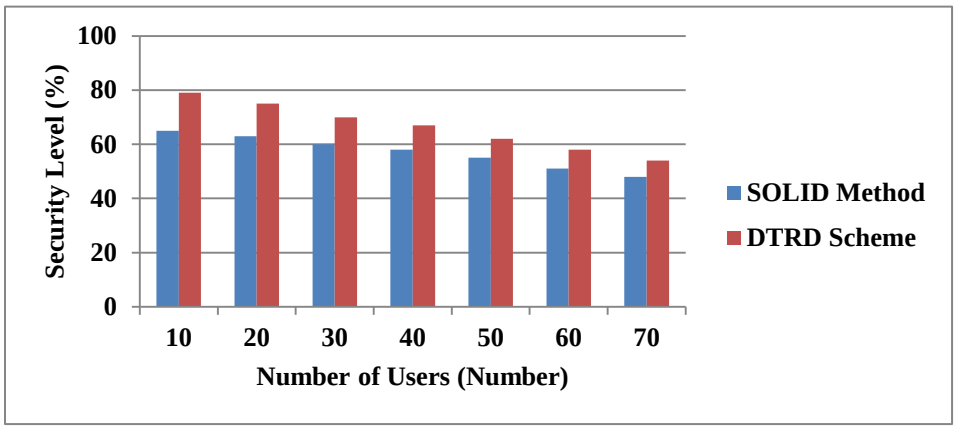

Fig. 4.3 Security Level on Authentication and Security Maintenance in WSN

Fig. 4.3 illustrates the security level of existing authentication and security maintenance techniques. Security level of Distributed token reuse detection (DTRD) Scheme is comparatively higher

than that of Sequential mOnte carLo combIned with shadow-faDing estimation (SOLID) method. Security level of DTRD scheme is 10-18% higher secure than SOLID Method.

4.4 ENERGY CONSUMPTION

Energy consumption is defined as amount of energy consumed while authenticating and maintaining the security of the user's data. It is measured in terms of Joules.

Number of Users (Number)	Energy Consumption (Joules)		
	VEBEK Scheme	MTTF Probabilistic System	Probabilistic Approach
10	52	65	45
20	56	69	48
30	59	72	50
40	62	75	53
50	65	79	57
60	69	81	60
70	73	85	63

Table 4.4 Tabulation for Energy Consumption on Authentication and Security Maintenance in WSN

The energy consumption comparison takes place on existing Virtual Energy-Based Encryption and Keying (VEBEK) scheme, Mean Time To Failure (MTTF) Probabilistic System, and Probabilistic Approach.

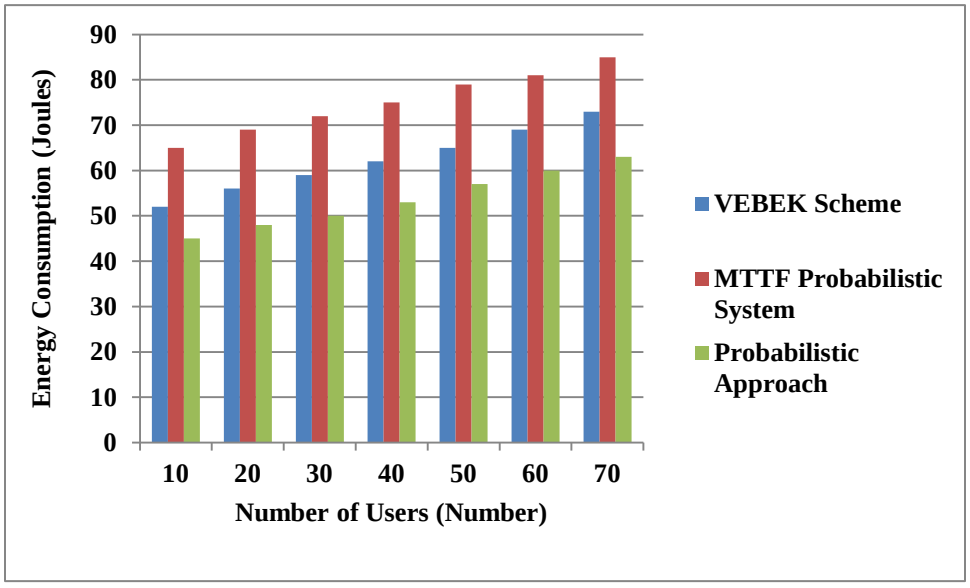

Fig. 4.4 Energy Consumption on Authentication and Security Maintenance in WSN

From fig. 4.4, energy consumption of existing systems on authentication and security maintenance techniques are described. Energy Consumption of Probabilistic Approach is comparatively lesser than that of Virtual Energy-Based Encryption and Keying (VEBEK) scheme and Mean Time To Failure (MTTF) Probabilistic System. Research in the energy consumption of Probabilistic approach is 12-16% lesser than that of Virtual Energy-Based Encryption and Keying (VEBEK) scheme and 35-45%higher than that of Mean Time To Failure (MTTF) Probabilistic System.

5. DISCUSSION ON LIMITATION OF AUTHENTICATION AND SECURITY MAINTANANCE IN WIRELESS NETWORKS

In probabilistic approach, malicious node's maxmin strategy corresponds to the optimal strategy is not proved. The approach fails to extend the framework to handle multiple malicious nodes. Additional security counter measures are also not carried out in the probabilistic approach. In Data Aggregation and Authentication protocol (DAA), key establishment process is more susceptible to node cooperation attacks. False data detection and data confidentiality enhances the communication overhead. Each sensor node can able to aggregate and forward data but does not improve network security and efficiency.

Virtual ring architecture fails to support the privacy protection mechanism with future resource computing environments. Network Security Architecture with ticket based protocol, client's bandwidth allocation depending on the logged data in log is not effective in sensor network. Many threats are occurred on the dynamic paths on Virtual Energy-Based Encryption and Keying (VEBEK) scheme. Distributed token reuse detection (DTRD) scheme for DP2AC under different attacker model is not investigated.

In Mean Time To Failure (MTTF) Probabilistic system cruel attacks happen with the packet dropping in sensor network. Also the multipath route decision intrusions take place in system. In Sequential mOntecarLo combIned with shadow-faDing estimation (SOLID) method, signal propagation is random and so the attack takes place in the system.

5.1 Future Directions

The future direction of authenticating and maintaining the security in wireless sensor networks can be in the following ways:

- Achieving high efficient bandwidth technique on reducing the gang injecting false data attack
- Improving the authentication scheme on sensor network by overcoming the false data injection
- Maintaining the system with high authentication scheme without any false data injection

6. CONCLUSION

Observation about the existing authentication and security maintenance in wireless sensor networks such as Data Aggregation and Authentication (DAA) protocol, Virtual Ring Architecture, NSA with ticket based Protocol, Virtual Energy-Based Encryption and Keying (VEBEK) scheme, Mean Time To Failure (MTTF) Probabilistic System, Probabilistic Approach, Distributed token reuse detection (DTRD) Scheme, and Sequential mOnte carLo combIned with shadow-faDing estimation (SOLID) method. Probabilistic approaches determine the reputation of the nodes and minimize the maximum deception of the malicious node. Malicious node is interested to change the positioning strategy in the attempt to masquerade itself.

In Virtual ring architecture, privacy protection solution aims to support all the aforementioned architectural design goals. Privacy of customers minimizes the performance overhead of cryptographic computations. The architecture also offers privacy protection in the smart grid environment. Data Aggregation and Authentication protocol combines false data detection with data aggregation and confidentiality. It is also employed to support confidential data transmission between two consecutive data aggregators to verify the data integrity on the encrypted data. DAA detects false data injected by a data aggregator to minimize the waste of resources such as bandwidth and battery power.

Network Security Architecture with ticket based protocol binds the ticket and pseudonym which guarantees anonymous access control. Also payment-based approach offers sufficient incentives for improving both cooperativeness and availability. VEBEK is a secure communication framework where sensed data is encoded using a scheme based on a permutation code created via the RC4 encryption mechanism. RC4 encryption alters function of the residual virtual energy of the sensor. VEBEK updates keys without exchanging messages for key renewals.

Distributed Privacy-Preserving Access Control scheme for sensor networks purchase tokens from the network owner. Query data from sensor nodes reply only after validating the tokens. DP2AC is detecting reused tokens and it is a random bit string with no relationship to user identities. Mean Time To Failure (MTTF) Probabilistic system handle running into energy exhaustion for the best case of processing. Dynamic redundancy management algorithm is used to identify and apply the design parameter settings at runtime in response to environment changes. The key idea underlying SOLID is to exploit the temporal shadow fading correlation in sensing results induced by the primary user's mobility. SOLID augments conventional Sequential Monte Carlo (SMC)-based target tracking with shadow-fading estimation.

Inspection was increasing the authentication and security maintenance level in wireless sensor networks on existing techniques. This helps to detect the malicious user to access the user's data. The wide range of experiments estimates the comparative performance of the various security maintenance and authentication techniques. Finally, the result shows that the security maintenance and authentication in WSN increases the privacy of the user's data over a wide range of experimental parameters.

REFERENCES

[1] Rongxing Lu., Xiaodong Lin., Haojin Zhu., Xiaohui Liang, and Xuemin (Sherman) Shen., "BECAN: A Bandwidth-Efficient Cooperative Authentication Scheme for Filtering Injected False Data in Wireless Sensor Networks," IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS, VOL. X, NO. X, XX 2010

[2] Suat Ozdemir., and Hasan Çam., "Integration of False Data Detection With Data Aggregation and Confidential Transmission in Wireless Sensor Networks," IEEE/ACM TRANSACTIONS ON NETWORKING, VOL. 18, NO. 3, JUNE 2010

[3] Nicola Basilico., Nicola Gatti., Mattia Monga., and Sabrina Sicari., "Security Games for Node Localization through Verifiable Multi-lateration," IEEE TRANSACTIONS ON DEPENDABLE AND SECURE COMPUTING, VOL. 11, and NO: 1, JANUARY/FEBRUARY 2014

[4] Jinyuan Sun., Chi Zhang., Yanchao Zhang., and Yuguang Fang., "SAT: A Security Architecture Achieving Anonymity and Traceability in Wireless Mesh Networks," IEEE TRANSACTIONS ON DEPENDABLE AND SECURE COMPUTING, VOL. 8, NO. 2, MARCH-APRIL 2011

[5] Arif Selcuk Uluagac., Raheem A. Beyah., Yingshu Li., and John A. Copeland., "VEBEK: Virtual Energy-Based Encryption and Keying for Wireless Sensor Networks," IEEE TRANSACTIONS ON MOBILE COMPUTING, VOL. 9, NO. 7, JULY 2010

[6] Rui Zhang., Yanchao Zhang., and Kui Ren., "Distributed Privacy-Preserving Access Control in Sensor Networks," IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS, VOL. 23, NO. 8, AUGUST 2012

[7] Hamid Al-Hamadi., and Ing-Ray Chen., "Redundancy Management of Multipath Routing for Intrusion Tolerance in Heterogeneous Wireless Sensor Networks," IEEE TRANSACTIONS ON NETWORK AND SERVICE MANAGEMENT, VOL. 10, NO: 2, JUNE 2013

[8] Alexander W. Min., and Kang G. Shin., "Robust Tracking of Small-Scale Mobile Primary User in Cognitive Radio Networks," IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS, VOL. 24, NO. 4, APRIL 2013

[9] Mohamad Badra., and Sherali Zeadally., "Design and Performance Analysis of a Virtual Ring Architecture for Smart Grid Privacy," IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, VOL. 9, NO: 2, FEBRUARY 2014

