International Journal of Engineering Science Invention (IJESI)
ISSN (Online): 2319 – 6734, ISSN (Print): 2319 – 6726
www.ijesi.org ||Volume 7 Issue 3 Ver. 4 || March 2018 || PP42-49

Diverse Types Of Network Attacks and the Describing Security Mechanisms

Madhava Rao K[1] And Prof. Ramakrishna S[2]
Department Of Computer Science, Svu College Of Cm & Cs,Tirupati-517502, A.P. India,
Corresponding Author: Prof. Ramakrishna S

***Abstract*:** *In The Current Scenario Networking Protocols Are Enormously Momentous To The Computer Users In Personal, Trade, Defence, Armed Forces Etc. By The Promising Of Internet, Security Of The Networks Became The Foremost Concern. Despite The Fact That Going Through The History We Can Evidently Understood The Development Of Networks Security With Time. Networks Have Grown In Both Size And Importance In A Very Less Period Of Time. Obviously Networks Are Very Much Important From Common Man To Organisation That Is From National To International Also They Are Very Much Prone To Attacks Due To Unsatisfactory Predictable Prevention Mechanisms, Vulnerabilities And Loopholes. If The Security Is Compromised, There May Perhaps Be Grave Consequences Preliminarily From Burglary Of Information, Loss Of Confidentiality And Yet Attaining Ruin Of The Particular Institution. At The Moment The Challenge As Regards Security Issue Is To Discover A Superior Balanced Circumstance Connecting Two Of The Most Indispensable Necessities. In This Paper We Explore Various Kinds Of Attacks On Networks And The Requisite Security Mechanism.*

***Keywords*:** *Authentication, Data Transformation, Integrity, Monitor, Privacy*

Date of Submission: 01-03-2018 Date of acceptance 23-03-2018

I. Introduction

By The Arrival Of Internet And Novel Networking Technology The World Is More And More Consistent And There Is A Large Quantity Of Information Of Individual, Commerce, Protection, And Government On Networking Infrastructures Overall [1,2]. As An Effect Of Advancing In Network Protocols, Over The Years The Tools And Methods Of Networks Have Also Been Appreciably Developed. Prior Attacker Ought To Have Sophisticated System, Programming And Networking Knowledge To Have Prime Tools But In The Present Days Things Have Been Altered Tools And Methods Of The Adversary Have Also Been Developed In Principal. Consequently No Longer Necessitate Of Such Complicated Level Of Knowledge. Security Is Crucial For Diverse Networks Applications, Networks Security Is Receiving Of Exceedingly Significance Due To Uncomplicated Mean Of Acquiring Intellectual Property Through The Internet. Nevertheless Security Is A Crucial Thing Of Obligation For The Growing Networks, There Is A Vast "Communication Gap" Between The Designers Of Security Technology And Developers Of Network Protocols. Network Security Concerns Not Only Securing The Computers At Every End Of Communication Chain, It Means Securing The Entire Communication Channel Where There Is A Likelihood Of Attack By The Adversary Decrypt The Communication And Inserts A Counterfeit Message.

II. Possibility Of Primary Security Schemes In Networks

Security Is A Commonly Used Word Concerning The Characteristics Of Authentication, Reliability, Privacy, Non Repudiation And Anti-Playback [3]. For The Intention Of Securing Communication Of Diverse Types Of Information Over Networks, A Variety Of Techniques Like Cryptographic, Steganographic Etc Are Used Which Are Well Recognized .A Few Vital Security Terminology Have Been Explained Evidently In The Following [2].

A) Access – Make Available The Means Of Communication To The Authorized Users From An Exacting Network

B) Authentication – Make Sure The Users Of The Network Are Who They Say They Are Or If Not

C) Confidentiality And Secrecy – Make Certain That The Information In The Network Is Privacy.

D) Integrity – Ensure That Alteration In The Communication Ought To Never Happen While Transit.

E) Non-Repudiation – Ensure That The User Never Refutes The Network He Used.

2.1 *Cryptography*

Cryptography Is Transmitting The Information In Undisclosed Coded Approach. At This Time In Cryptography The Content Of The Communication Is In Hide From View. On The Other Hand The Techniques Of Encryption-Decryption Are Devised For The Conventional Wired Networks Not Potential To Be Applied Directly For The Wireless Networks. Wireless Networks Consist Of Minute Sensors Which Truly Suffer From The Lack Of Processing, Memory And Battery Power [4-8].Therefore Extra Processing, Extra Memory And Extra Battery Power Are The Required For The Application Of Encryption Technique.

2.2 Steganography

Where As Cryptography Aims At Hiding The Content Of The Message, Steganography [9,10] Aims At Hiding The Being Of The Message. Steganography Is The Art Of Hidden Communication By Embedding A Message Into The Multimedia Data In The Form Of Image, Sound, Video, Etc.[11]. Considerably This Method Is Used In The Situation Where There Is A Need Of Conveying The Undisclosed Data Publicly.

III. Diverse Kinds Of Attacks In Networks

Obviously The Attacks Occurred In The Physical Layer Are Jamming And Tampering [12].When An Attacker Blocks The Radio Frequencies That Are Using By Legitimate Sensor Nodes Then Jamming Will Take Place. Otherwise If The Attacker Blocks The Complete Network A Whole Denial Of Service (Dos) Occurs. Tampering Is Material Damage That Is Alteration Or Replacement Of Either A Node Or Part Of A Node. Sensors Damage, Modification Or Alteration Of Circuitry, Changing Of Hardware Of The Node Or Of The Entire Node, And Altering Of Sensors With Malicious Sensors Are Examples Of Tampering. In Additional To, An Attacker Can Cross Examine The Nodes Electronically To Get Hold Of Access To Cryptographic Data And The Information Which Is Going To Access On Other Communication Layers. Major Attacks Are Explaining Visibly In The Below With Separate Headings.

3.1 Denial Of Service (Dos)

Obviously This Will Happen By The Unintentional Or Unplanned Failure Of Nodes Or Malicious Action [13, 14]. The Simple Dos Attack Try To Drain The Resources Which Are Accessible To The Victim Node, Through Transfer Of Unnecessary Extra Packets, As A Result Prevents Authorized Network Users From Available Services To Which They Are Entitled. Dos Attack Intended Not Only For The Attacker's Effort To Subvert, Interrupt, Or Demolish A Network, But Also For Any Incident That Destroy Network's Facility To Make Available A Service. Quite A Few Types Of Dos Attacks Are Performed In Different Layers. At Physical Layer Jamming And Tampering Could Be Performed, At Link Layer, Collision, Exhaustion, Unfairness, At Network Layer, Ignore And Greed, Homing, Misdirection, Black Holes And At Transport Layer Attack Might Be Performed By Malicious Flooding.

3.2 Attacks On Information In Transit

Obviously In A Sensor Network, The Variations Of Specific Parameters Or Values Monitor By Sensors And Then Inform To The Sink Based To The Requirement. At The Time Of Transferring The Report, The Information In Transit Might Be Changed, Deceived, Replayed Again Or Missing Will Takes Place. As We Know Networks Are Vulnerable To Eavesdropping, Adversary Can Observe Or Listen The Networked Messages Or Might Interfere To Break Off, Intercept, Vary Or Formulate The Packets Consequently Providing Counterfeit Information Or Data To The Destiny Stations Or Sinks [15].

3.3 Sybil Attack

In A Sensor Network The Sensors Might Have To Work In Concert To Complete A Task In Some Conditions Consequently They Can Use Allocation Of Subtasks And Redundant Of Information. In Such A State, A Node Can Act As If To Be More Than One Node Using The Identities Of Other Authorized Nodes. This Kind Of Attack Where As A Node Forges The Identities Of More Than One Node Is Sybil Attack [16, 17].

3.4 Black Hole Attack Or Sink Hole Attack

In This Attack, The Aim Is To Lure All The Traffic To A Malicious Node Of The Network [18]. It Is Achievable By Making Of A Compromised (Malicious) Node Appear Alluring To Its Neighbors In Terms Of Routing Of Packets. Particularly In A Flooding Based Protocol, The Adversary Listens To Requests For Routes And Replies The Target Node That It Encompass The Large Quality Or Shortest Path To The Base Station. Once The Compromised Node Is In A Position To Place In Itself Connecting The Communicating Nodes Then It Is Capable Of Doing Whatever With The Packets Passing Between Them. Actually, This Might Affect Even The Nodes That Are Significantly Far From The Base Stations.

3.5 Hello Flood Attack

This Attack Uses The Hello Packets As A Weapon To Induce The Sensors In Sensor Network. In This Type Of Attack An Adversary With A Large Radio Communication (Laptop-Class Attacker In [19]) Range And Processing Power Transmit Hello Packets To More Number Of Sensor Nodes Which Are Scattered In A Large Area Within A Sensor Network. The Sensors As A Result Convinced The Attacker Is Their Neighbor. As An Outcome, While Transferring The Data To The Base Station, The Victim Nodes Try To Go Through The Adversary As They Know It Is Their Neighbor And Are Eventually Deceived By The Adversary.

3.6 Wormhole Attack

Wormhole Attack Is A Significant Attack, In This Attack Adversary Records The Packets At One Locality Or Spot In The Network And Tunnels Or Retransmits These To Another Locality [20]. The Retransmitting Of Packets Might Be Made Selectively. This Attack Is A Considerable Threat To Wireless Sensor Networks [Wsn], For The Reason That This Type Of Attack Does Not Necessitate Compromising A Sensor In The Networks Rather; It Could Be Performed Yet At The Primary Phase When The Sensors Begin To Find Out The Neighboring Information.

IV. Security Mechanisms For Sensor Networks

An Analysis Of Secure Routing In Wireless Sensor Networks [Wsn]Is Given In[19], [21] Gives The Approach To Develop Secure Dispersed Sensor Networks With Numerous Supply Voltages To Decrease The Energy Spending On Computation And Consequently To Extend The Network's Life Span. [22] Aims At Mounting Energy Efficiency For Key Management In Sensor Networks And Uses The Network Model For Its Application [23]. [24] Shows The Dos Attacks Next To Various Layers Of Sensor Protocol Stack. In [25] Jam Gives A Mapping Protocol Which Finds A Jammed Area In The Sensor Network And Helps To Keep Away From The Defective Section To Keep On Routing Within The Network, Consequently Handles Dos Attacks Occurred By Jamming. Wormholes That Are So Far Deemed Detrimental For Wsn Could Efficiently Be Used As A Reactive Defense Mechanism For Preventing Jamming Dos Attacks [26]. Statistical En-Route Filtering (Sef) Method Is Used To Identify Injected Fake Data In Sensor Networks And Focus Principally On How To Filter Fake Data Using Collective Undisclosed And Accordingly Checking Any Single Compromised Node From Breaking The Whole System [27]. Snep & µtesla Are Major Secure Building Blocks For Providing Data Privacy, Data Originality And Broadcast Authentication [28]. Tinysec Proposes A Link Layer Security Scheme For Sensor Networks Which Uses An Capable Symmetric Key Encryption Protocol [19]. Article [17] Gives A Few Defense Mechanisms Against Sybil Attack In Sensor Networks. Analysis The Problem Of Assigning Primary Secrets To Users In Ad-Hoc Sensor Networks To Make Sure Authentication And Confidentiality Throughout Their Communication And Points Out Potential Ways Of Giving Out The Secrets Has Been Mentioned In [29]. Article [30] Shows A Probabilistic Undisclosed Sharing Protocol To Protect Hello Flood Attacks. The Mechanism Uses A Bidirectional Authentication Technique And Also Introduces Multi-Path Multi-Base Station Routing If Bidirectional Verification Is Not Adequate To Secure The Attack.

V. Architecture Of Classification Of Attacks

The Architecture Of General Classification Of Network Attacks Has Been Explained In Fig.1 After An Obvious Explanation Of Few Words Involved In The Architecture.

Eavesdropping And Passive Monitoring: This Is Hugely Widespread And Simple Form Of Attack On Data Confidentiality. If The Communication Is Not Protected By Cryptographic Mechanisms, The Attacker Might Easily Be Aware Of The Contents. Packets Or Bits Consisting Of Control Information In A Sensor Networks Transmit Large Information Than Available Through The Location Server, Eavesdropping On These Messages Prove High Useful For An Attacker.

Traffic Analysis: In Order To Put Up An Effectual Attack On Confidentiality, Eavesdropping Could Be Combined With A Traffic Analysis. By An Effectual Analysis Of Traffic, An Attacker Can Recognize Some Sensor Nodes With Special Tasks And Activities In Sensor Networks. For Instance, An Unexpected Enhance In Message Communication Connecting Certain Nodes Signifies That These Nodes Have Some Exact Activities And Proceedings To Monitor. The Demonstration Of Two Types Of Attacks That Can Discover The Base Station In A Sensor Networks With No Even Underrating The Contents Of The Packets Or Bits Being Analyzed In Traffic Analysis [31].

Camouflage: An Attacker Might Compromise A Sensor Node In A Sensor Networks And In A While Use That Node To Deception A Regular Node In The Network. This Camouflaged Node Then Might Broadcast

Fake Routing Information And Attract Packets Or Bits From New Nodes For Further Forwarding. After The Packets Begin Incoming At The Compromised Node, It Starts Forwarding Them To Intentional Nodes Where Confidential Analysis On The Packets Might Be Passed Out Systematically.

Viruses: These Are Self-Replication Programs Infect The Files And Propagate, Once A File Is Disclosed, The Virus Will Activate In To The System [32].

Worms: A Worm Is Analogous To A Virus As They Both Are Self-Replicating, However The Worm Never Need A File To Allow It To Propagate [32]. Two Major Types Of Worms Are There, Mass-Mailing Worms And Network Aware Worms. Mass Mailing Worms Use Email As A Way To Infect Other Computers. Network-Aware Worms Are A Most Important Problem For The Internet. A Network-Aware Worm Selects A Target And Once The Worm Accesses The Target Host, It Can Infect It By Means Of A Trojan Or Otherwise.

Trojans: Trojans Emerge To Be Benign Programs To The User, However Will Really Have Some Malicious Purpose. Trojans Generally Transmit Some Payload Such As A Virus [32].

Node Subversion: Capture Of A Node Might Disclose Its Information As Well As Revelation Of Cryptographic Keys And As A Result Compromise The Entire Sensor Network. A Specific Sensor May Be Captured, And Information That Is Key Stored On It May Get By An Attacker. [33]

Node Malfunction: A Malfunctioning Node Will Create Incorrect Data That Might Represent The Integrity Of Sensor Network In Particular If It Is A Data-Aggregating Node Such As A Cluster Leader [33].

Node Outage: When A Node Stops Its Function Then This Situation, Node Outage Is Possible To Occur. In This Case Where As Cluster Leader Stops Performing, The Sensor Network Protocols Must Be Robust Enough To Moderate The Effects Of Node Outages By An Alternate Route [33].

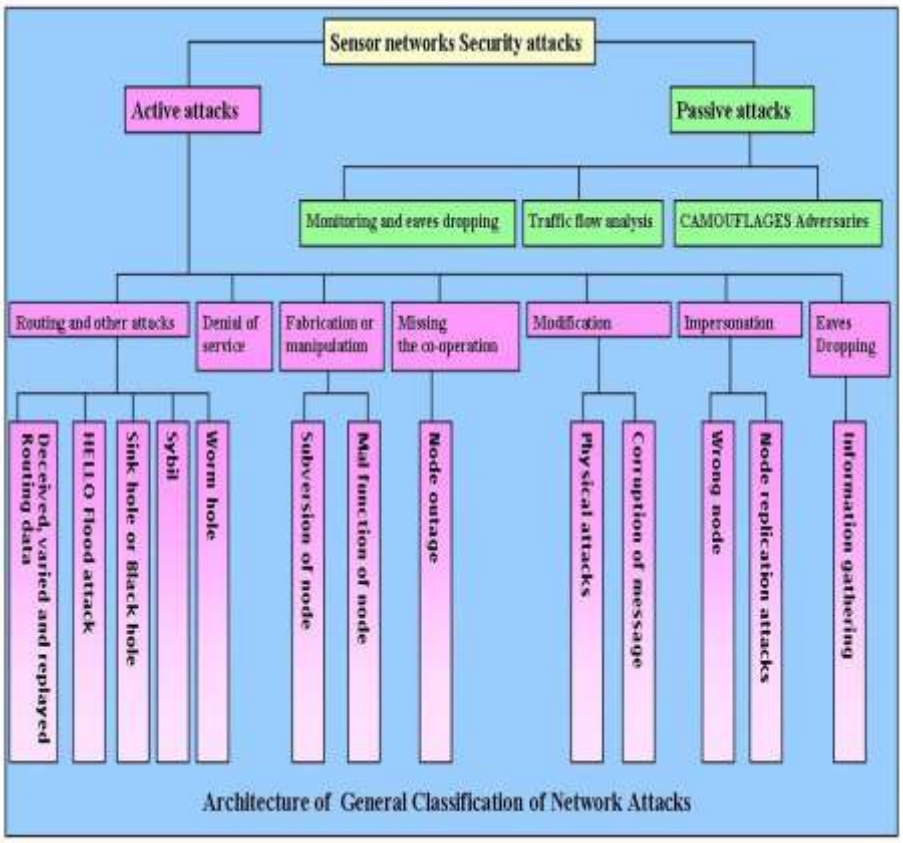


Fig.1

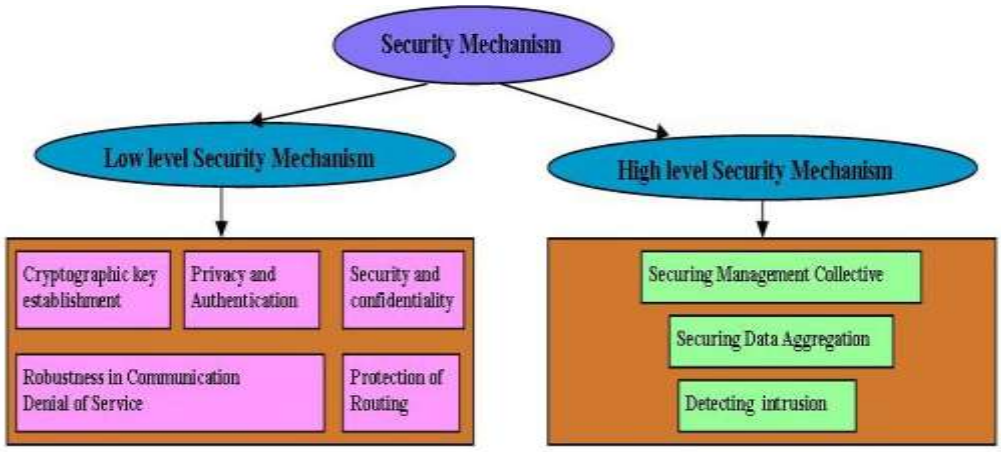
Message Corruption: Any Alteration Of The Content Of A Communication By An Adversary Compromises Its Reliability Or Integrity [34]

False Node: A Fake Node Involves The Adding Up A Node By A Challenger And Causes The Insertion Of Malicious Data. An Interloper May Add A Node To The System That Includes Bogus Data Or Restricts The Route Of True Data. Inclusion Of Malicious Node Is One Of The Most Hazardous Attacks That Can Takes Place. Malicious Code Injected In The Network Might Extend To All Nodes, Significantly Destroying The Entire Network, Or Yet Worse, Taking Over The Network On Behalf Of A Challenger [34].

Node Replication Attacks: Conceptually, A Node Replication Attack Is Somewhat Simple; An Adversary Seeks To Link Up A Node To An Accessible Sensor Network By Replicating The Node Id Of An Accessible Sensor Node. A Node Simulated In This Approach Can Severely Interrupt Sensor Network's Performance. Packets Be Able To Corrupt Or Yet Misrouted. Consequently Network Disconnection, Fake Sensor Readings, Etc. Will Happen. If An Adversary Can Put On Physical Access To The Entire Network He Be Able To Copy Cryptographic Keys To The Simulated Sensor Nodes. By Introducing The Simulated Nodes An Exact Network Points, The Attacker Might Easily Operate A Definite Segment Of The Network, Possibly By Disconnecting It Overall [35].

VI. Architecture Of The Required Security Mechanism

The Architecture Of Necessitate Security Mechanism Has Been Given In Fig.2 Following This Terms In Architecture Is Explained In An Insight Manner.



Architecture of Classification of Security Mechanism

Fig.2

Low-Level Mechanism: Primary Issues For Securing Sensor Networks In Low-Level Mechanism Are,
A. Cryptographic Key Establishment And Trust Setup
B. Privacy And Authentication
C. Secrecy And Confidentiality
D. Robustness In Communication Denial Of Service
E. Protection Of Routing
F. Resilience Or Flexibility To Node Capture

Cryptographic Key Establishment And Trust Setup: The Crucial Requisite For Setting Up The Sensor Network Is The Founding Of Cryptographic Keys. By And Large The Sensor Devices Have Inadequate Computational Power And The Public Key Cryptographic Primitives Are Very Expensive To Go After. Key-Establishment Techniques Have To Scale To Networks With Hundreds Or Thousands Of Nodes. In Addition, The Communication Patterns Of Sensor Networks Vary From Conventional Networks; Sensor Nodes Might Require To Set Up Keys With Their Neighbors And With Data Aggregation Nodes. The Drawback Of This Approach Is That Attackers Who Compromised Adequately And Many Nodes Might Also Renovate The Whole Key Collection And Crack The Scheme [35].

Privacy And Authentication: Most Of The Sensor Network Applications Necessitate Defense Against Eavesdropping, Insertion, And Alteration Of Packets. Cryptography Is The Regular Security. Notable System Trade-Offs Come Up When Incorporating Cryptography Into Sensor Networks. For Point-To-Point Communication Uninterrupted Cryptography Achieves A High Level Of Protection However Require That Keys Be Set Up Among All End Points And Be Unable To Coexist With Passive Involvement And Home Broadcast [36]. Link-Layer Cryptography With A Network Extensive Shared Key Simplifies Key Setup And Supports Passive Participation And Home Broadcast, But Middle Nodes Might Eavesdrop Or Modify Messages. The Primitive Sensor Networks Are Likely To Use Link Layer Cryptography, For The Reason That This Approach Provides The Utmost Simplicity Of Deployment Among Currently Available Network Cryptographic Means [33].

Secrecy And Confidentiality: Be Fond Of Other Conventional Networks, The Sensor Networks Have Also Compelled Confidential Concerns. In The Beginning The Sensor Networks Are Deployed For Legitimate Purpose Could Afterward Be Used In Unanticipated Ways. As Long As Awareness Of The Existence Of Sensor Nodes And Data Acquisition Is Predominantly Essential [35].

Robustness In Communication Denial Of Service: A Hacker Attempts To Interrupt The Network's Function By Propagating A High-Energy Signal. If The Broadcast Is Powerful Adequate, The Whole System's Communication Might Be Jammed. Extra Complicated Attacks Are Also Feasible, The Hacker Could Inhibit Communication By Violating The802.11 Medium Access Control (Mac) Protocol By, Say To, Transmitting Whereas A Neighbor Is Also Transmitting Or By Incessantly Requesting Channel Access With A Request-To Send Signal [35].

Protection Of Routing: Steering And Data Forwarding Is A Decisive Service For Enabling Communication In Sensor Networks. Sorry To Say, Current Routing Protocols Suffer From Lots Of Security Vulnerabilities. For Example, A Hacker May Start On Denial Of- Service Attacks On The Routing Protocol, Preventing Communication. The Simplest Attacks Engage Injecting Malicious Routing Information Into The Network, Ensuing In Routing Inconsistencies. Uncomplicated Authentication Possibly Will Guard.

Table 1: Different Types Of Network Attacks , Required Security Mechanisms And Major Features Are Summarized In The Below Table

S.No	Network Attacks	Security Mechanisms	Major Features
1	Dos Attack (Jamming)	Jam [25]	Prevention Of Jammed Region By Using Coalesced Neighbor Nodes
2	Dos Attack (Jamming)	Wormhole Based [26]	Uses Wormholes To Keep Away From Jamming
3	Information Deceiving	Statistical En-Route Filtering [27]	Detects And Drops Fake Reports During Forwarding Process
4	Sybil Attack	Radio Resource Testing, Random Key Pre-Distribution Etc. [19]	Uses Radio Resource, Arbitrary Key Pre Distribution, Registration Process, Position Confirmation And Code Evidence For Detecting Sybil Entity
5	Hello Flood Attack	Bidirectional Verification, Multi-Path Multi-Base Station Routing [29]	Adopts Probabilistic Undisclosed Sharing, Uses Bidirectional Confirmation And Multi-Path Multi-Base Station Routing
6	Information Or Data Deceiving	On Communication Security [40]	Competent Resource Management, Secures The Network Yet If Part Of The Network Is Compromised
7	Information Spoofing Or Data Spoofing And Wormhole Attack	Tik [37]	Depends On Symmetric Cryptography, Requires Exact Time Synchronization Among All Communicating Parties, Implements Temporal Leashes
8	Attacks In Information In Transit And Data And Information Deceive	Random Key Pre Distribution [38], [39], [42]	Make Available Resilience Of The Network, Protect The Network Even If Part Of The Network Is Compromised, Provide Authentication Measures For Sensor Nodes
9	Data And Information Spoofing	[43]	Suitable For Large Wireless Sensor Networks Which Allows Accumulation And Removal Of Sensors, Resilient To Sensor Node Capture
10	Blackhole Attacks	Reward [44]	Uses Geographic Routing, Takes Benefit Of The Broadcast Inter-Radio Performance To Watch Neighbor Transmissions And Discover Black Hole Attacks
11	Data And Information Deceiving, Message Replay Attack	Tinysec [41]	Focuses On Giving Message Legitimacy, Reliability And Confidentiality, Works In The Link Layer
12	Data Spoofing And	Snep & µtesla [28]	Semantic Security, Data

	Information Spoofing, Message Replay Attacks		Authentication, Replay Protection, Weak Freshness, Low Communication Overhead

VII. Conclusion

Network Security Is A Vital Field That Is More And More Gaining Attention As The Internet Expands. The Security Fear And Internet Protocol Were Analyzed To Find Out The Required Security Technology. The Security Technology Is Typically Software Based, However Lots Of General Hardware Devices Are Used. The Existing Development In Network Security Is No Very Extraordinary. This Paper Summarizes The Attacks And Their Classifications In Sensor Networks And Also An Effort Has Been Made To Investigate The Security Mechanism Extensively Used To Handle Those Attacks. This Survey Will Optimistically Stimulate Future Researchers To Come Up With Smarter And Additional Vigorous Security Mechanisms And Make Their Network Safe.

References

[1]. Main Types Of Attacks In Wireless Sensor Networks Teodor-Grigore Lupu* *Department Of Computer And Software Engineering University "Politehnica" Of Timisoara, Faculty Of Automatics And Computers Vasile Parvan 2, 300223, Timisoara Romania E-Mail: Teodor.Lupu@Hd.Politiaromana.Ro

[2]. Blessy Rajra M B, A J Deepa, A Survey On Network Security Attacks And Prevention Mechanism, Journal Of Current Computerscience And Technology, 5(2), February 2015 2231-5411

[3]. Undercoffer, J., Avancha, S., Joshi, A., And Pinkston, J., Security For Sensor Networks, Cadip Research Symposium, 2002

[4]. Al-Sakib Khan Pathan Department Of Computer Engg. Kyung Hee University, Korea Spathan@Networking.Khu.Ac.Kr , Hyung-Woo Lee Department Of Software, Hanshin University, Korea, Hwlee@Hs.Ac.Kr, Choong Seon Hong Department Of Computer Engg. Kyung Hee University, Korea, Cshong@Khu.Ac.Kr, Security In Wireless Sensor Networks: Issues And Challenges

[5]. Perrig, A., Szewczyk, R., Wen, V., Culler, D., And Tygar, J. D., Spins: Security Protocols For Sensor Networks, WirelessNetworks,8(5),2002, 521-532

[6]. Jolly, G., Kuscu, M.C., Kokate, P., And Younis, M., A Low-Energy Key Management Protocol For Wireless Sensor Networks, Proc. Eighth Ieee International Symposium On Computers And Communication, 1,2003 335 - 340.

[7]. Rabaey, J.M., Ammer, J., Karalar, T., Suetfei Li., Otis, B., Sheets, M., And Tuan, T., Picoradios For Wireless Sensor Networks: The Next Challenge In Ultra-Low Power Design, Ieee International Solid-State Circuits Conference,1, 2002, 200 –201

[8]. Hollar, S, Cots Dust, Master's Thesis, Electrical Engineering And Computer Science Department, Uc Berkeley, 2000.

[9]. Kurak, C And Mchugh, J, A Cautionary Note On Image Downgrading In Computer Security Applications, Proceedings Of The 8th Computer Security Applications Conference, San Antonio, 1992, 153-159.

[10]. Mokowitz, I. S., Longdon, G. E., And Chang, L., A New Paradigm Hidden In Steganography, Proc. Of The 2000 Workshop On New Security Paradigms, Ballycotton, County Cork, Ireland, 2001, 41– 50.

[11]. Kim, C. H., O, S. C., Lee, S., Yang, W. I., And Lee, H-W., Steganalysis On Bpcs Steganography, Pacific Rim Workshop ODigital Steganography (Steg'03), July 3-4, Japan , 2003.

[12]. Kaplantzis, S.Supervisors Dr, N. Mani, Prof. M.Palaniswami, Prof G. Egan. Security Models For Wireless Sensor Networks. Citeseerx: 10.1.1.87.4605, 2006. Available: Http://Members. Iinet.Com.Au/~Souvla/Transfer-Final-Rev.Pdf

[13]. Blackert, W.J., Gregg, D.M., Castner, A.K., Kyle, E.M., Hom, R.L., And Jokerst, R.M., Analyzing Interaction Between Distributeddenial Of Service Attacks And Mitigation Technologies, Proc. Darpa Information Survivability Conference And Exposition, 1, 2003, 26 – 36.

[14]. Wang, B-T. And Schulzrinne, H., An Ip Traceback Mechanism For Reflective Dos Attacks, Canadian Conference On Electrical And Computer Engineering, 2, 2004, 901– 904.

[15]. [Pfleeger, C. P. And Pfleeger, S. L., Security In Computing, 3rd Edition, Prentice Hall, 2003.

[16]. Douceur, J. The Sybil Attack, 1st International Workshop On Peer-To-Peer Systems , 2002

[17]. Newsome, J., Shi, E., Song, D, And Perrig, A, The Sybil Attack In Sensor Networks: Analysis & Defenses, Proc. Of The Third International Symposium On Information Processing In Sensor Networks, Acm, 2004, 259 – 268

[18]. Culpepper, B.J. And Tseng, H.C., Sinkhole Intrusion Indicators In Dsr Manets, Proc. First International Conference On Broad Band Networks, 2004, 681 – 688.

[19]. Karlof, C. And Wagner, D., Secure Routing In Wireless Sensor Networks: Attacks And Countermeasures, Elsevier's Ad Hoc Network Journal, Special Issue On Sensor Network Applications And Protocols, 2003, 293-315.

[20]. Hu, Y.-C., Perrig, A., And Johnson, D.B., Packet Leashes: A Defense Against Wormhole Attacks In Wireless Networks, Twenty-Second Annual Joint Conference Of The Ieee Computer And Communications Societies. Ieee Infocom 2003, 3, 2003, 1976 – 1986.

[21]. Yuan, L. And Qu, G., Design Space Exploration For Energy-Efficient Secure Sensor Network, Proc. The Ieee International Conference On Application-Specific Systems, Architectures And Processors, 2002, 88 – 97.

[22]. Jolly, G., Kuscu, M.C., Kokate, P., And Younis, M., A Low-Energy Key Management Protocol For Wireless Sensor Networks, Proc.Eighth Ieee International Symposium On Computers And Communication, 1, 2003. 335 - 340.

[23]. Younis, M., Youssef, M., And Arisha, K., Energy-Aware Routing In Cluster-Based Sensor Networks, Proc. 10th Ieee International Symposium On Modeling, Analysis And Simulation Of Computer And Telecommunications Systems, 1-16 Oct. 2002 Pp. 129 – 136.

[24]. Wood, A. D. And Stankovic, J. A., Denial Of Service In Sensor Networks, Computer, 35, Issue 10, Oct. 2002 Pp. 54 - 62.

[25]. Wood, A.D., Stankovic, J.A., And Son, S.H., Jam: A Jammed-Area Mapping Service For Sensor Networks, 24th Ieee Real- Time Systems Symposium, Rtss, 2003, 286-297.

[26]. Cagalj, M., Capkun, S., And Hubaux, J-P., Wormhole-Based Anti-Jamming Techniques In Sensor Networks From Http://Lcawww.Epfl.Ch/Publications/Cagalj/Cagaljch05-Worm.Pdf

[27]. Ye, F., Luo, H., Lu, S, And Zhang, L, Statistical En-Route Filtering Of Injected False Data In Sensor Networks, Ieee Journal On Selected Areas In Communications,23(4), 2005, 839 – 850.

[28]. Perrig, A., Szewczyk, R., Wen, V., Culler, D., And Tygar, J. D., Spins: Security Protocols For Sensor Networks, Wireless Networks, 8(5), 2002, 521-534.

[29]. Kulkarni, S. S., Gouda, M. G., And Arora, A., Secret Instantiation In Adhoc Networks, Special Issue Of Elsevier Journal Of Computer Communications On Dependable Wireless Sensor Networks, 2005, 1–15
[30]. Hamid, M. A., Rashid, M-O., And Hong, C. S., Routing Security In Sensor Network: Hello Flood Attack And Defense, To Appear In Ieee Icnews, Dhaka. 2006, 2-4
[31]. Deng, J., R. Han, And S. Mishra, Countermeasures Against Traffic Analysis In Wireless Sensor Networks, Technical Report Cu-Cs-987-04, University Of Colorado At Boulder, 2004.
[32]. Tahirnaeem, Kok-Keong Loo, Common Security Issues And Challenges In Wireless Sensor Networks And Ieee 802.11 Wireless Mesh Networks, International Journal Of Digital Content Technology And Its Applications, 3, 2009, 89-90
[33]. John Paul Walters, Zhengqiang Liang, Weisong Shi, Vipinchaudhary, "Wireless Sensor Network Security: A Survey", Security In Distributed, Grid And Pervasive Computing Yang Xiao (Eds), 2006, 3-5, 10-15
[34]. Undercoffer, J., Avancha, S., Joshi, A. And Pinkston, J., Security For Sensor Networks, In Proceedings Of The Cadip Research Symposium, University Of Maryland, Baltimore County, Usa, 2002 Http://Www.Cs.Sfu.Ca/~Angiez/Personal/Paper/Sensor-Ids.Pdf
[35]. Adrian Perrig, John Stankovic, David Wagner, Security In Wireless Sensor Networks, Communications Of The Acm, 2004, 53-57
[36]. Dowd, P.W.; Mchenry, J.T., Network Security: It's Time To Take It Seriously, Computer, 31(9), 1998, 24-28
[37]. Hu, Y.-C., Perrig, A., And Johnson, D.B., Packet Leashes: A Defense Against Wormhole Attacks In Wireless Networks, Twenty-Second Annual Joint Conference Of The Ieee Computer And Communications Societies. Ieee Infocom 2003, Vol. 3, 30 March-3 April 2003, 1976 –1986.
[38]. Du, W., Deng, J., Han, Y. S., And Varshney, P. K., A Pairwise Key Pre-Distribution Scheme For Wireless Sensor Networks, Proc. Of The 10th Acm Conference On Computer And Communications Security, 2003, 42-51.
[39]. Oniz, C. C, Tasci, S. E, Savas, E., Ercetin, O., And Levi, A, Sefer: Secure, Flexible And Efficient Routing Protocol For Distributed Sensor Networks, From Http://People.Sabanciuniv.Edu/~Levi/Sefer_Ewsn.Pdf
[40]. Slijepcevic, S., Potkonjak, M., Tsiatsis, V., Zimbeck, S., And Srivastava, M.B., On Communication Security In Wireless Ad-Hoc Sensor Networks, 11th Ieee International Workshops On Enabling Technologies: Infrastructure For Collaborative Enterprises, 2002, 10-12 June 2002, 139 – 144.
[41]. Karlof, C., Sastry, N., And Wagner, D., Tinysec: A Link Layer Security Architecture For Wireless Sensor Networks, Proc. Of The 2nd International Conference On Embedded Networked Sensor Systems, Baltimore, Md, Usa, 2004, 162 – 175.
[42]. Chan, H, Perrig, A., And Song, D., Random Key Predistribution Schemes For Sensor Networks, In Ieee Symposium On Security And Privacy, Berkeley, California, 2003, 197–213.
[43]. Eschenauer, L. And Gligor, V. D., A Key-Management Scheme For Distributed Sensor Networks, Proc. Acm Ccs'02, 2002, 41-47
[44]. Karakehayov, Z., Using Reward To Detect Team Black-Hole Attacks In Wireless Sensor Networks, In Workshop On Real-World Wireless Sensor Networks (Realwsn'05), Stockholm, Sweden, 2005.

Madhava Rao K"Diverse Types Of Network Attacks And The Describing Security Mechanisms"International Journal of Engineering Science Invention (IJESI), vol. 07, no. 03, 2018, pp42-49