

Name

Description

cs.
  
g

SPTK1

To follow this tactic the Cumulative-Sum-based Intrusion Prevention System (CSIPS) can be applied. It which detects malicious behaviors, attacks and distributed attacks launched to remote clients and local hosts based on the Cumulative Sum (CUSUM) algorithm [p5]. In addition to the use of IPS the [p71 describes the use of Intrusion Detection Systems (IDS) techniques proposed for detecting the presence of jammers and numerous mechanisms which attempt to protect the network from jamming attacks.

P5
  
P7



SPTK2

Bootstrapping is a process in which one device is associated or connected with a part of network or similar devices. During the bootstrapping phase, a unique identity and other security parameters are associated with each device/thing. Secure bootstrapping ensures that only authenticated devices access the network. The simplest mechanism for carrying out the initial setup (security parameters, node identity) is via physical interface (USB, wire, chip contact, etc). Wifeless bootstrapping may lead to eavesdropping although it can be avoided by using

advanced cryptographic mechanisms which provide confidentiality. To optimize the key distribution mechanism, several key management schemes have been proposed in literature for WSNs [p6], to support secure communication and authentication among WSNs devices.

P6



SPTK3 Smart

Antennas

The [p47] proposed the use of smart antennas against malicious eavesdroppers. The [p47] proposed a suite of strategies that use arrays of arrays to provide considerable reductions in the exposure region. Exposure region that refers to the area within which an eavesdropper can access and decode the signals being transmitted. More details in [p47].

P47

SPTK4

Like traditional networks, wireless sensors applications require protection against eavesdropping, alteration, and packet injection. In order to achieve this protection, data cryptography can prevent these security issues. The [p48] describe countermeasures that can be applying to IoT.

P48



SPTK5

Authentication and the integrity of the software on the device should be verified using cryptographic hash algorithms, which would provide digital signatures. However, because of the low processing power on most of the devices and their need for ultra-low power consumption most cryptographic hash algorithms cannot be implemented, apart from NH and WH cryptographic hash functions that are optimal for ultra-low power consumption devices.

P60

00

0to-

sa. .m a

0 >,

0 0 ac

rn .2 P.

SPTK6

When a new device is introduced to the network, it should authenticate itself before receiving or transmitting data, to ensure it is identified correctly before authorization and keeping malicious devices out of the system.

P60



Q

SPTK7

Error detection mechanisms should be provided at each device, to ensure no tampering of sensitive data occurs. Low power consumption mechanisms like Cyclic Redundancy Checks (CRC), Checksum, Parity Bit are preferred, but for more secure error detection method WH

,oga IpiLic hash function should be applied.

P60



SPTK8

All RFID Tags, IDs and data should be encrypted on each device before transmission of

data to ensure confidentiality. However, because of the ultra-low power consumption, strong cryptographic encryption functions like AES cannot be implemented. Instead Blowfish

or RSA have lower power consumption and less processing power and can be successfully implemented on the physical layer devices.

P60



SPTK9

In some cases hiding sensitive information like the location and identity of nodes is crucial.

Although Zero-Knowledge approach would be the optimal solution for anonymity, it cannot be implemented on low power devices as it is a very strong algorithm and needs a lot of processing power,, hence K- anonymity approach best fits the job for low power devices such as the devices used in an IoT system.

P60



SPTK10

Data privacy in Network Layer

Illegal access to the sensor nodes can be prevented, using authentication mechanisms and point to point encryption.

P60

SPTK11

Routing security in Network Layer

Secure routing is vital to the acceptance and use of sensor networks for many applications,

but the majority of used routing protocols are insecure. However, security of routing can be ensured by providing multiple paths for the data routing which improves the ability of the system to detect an error and keep performing upon any known of failure in the system. Also, encryption and authentication mechanisms increase the security level of routing data.

P60

SPTK12

Data integrity in Network Layer

Using cryptographic hash functions, the integrity of the data received on the other end is confirmed. In case of prove of tampering of data, error correction mechanisms could be introduced to mitigate the problem.

P60

SPTK13

Data security in App Layer

Authentication Encryption and Integrity mechanisms are critical at this level for insuring the

privacy of the whole system and protecting against data theft; it prevents unauthorized access to the system and ensures the confidentiality of the system data.

P60

SPTK14

Setting up policies and permissions of who can access and control the IoT system, is a crucial part as this ensures the privacy of the data, and the well being of the system. ACLs can block or allow incoming or outgoing traffic, and give or block access to requests from different users inside or outside of the network.

P60

Access Control Lists in App Layer

SPTK15

Firewalls in App Layer

This is an extra effective layer of security that will help block attacks that authentication, encryption and ACLs would failed to do so. Authentication and encryption passwords can be broken if weak passwords were selected. A firewall can filter packets as they are received, blocking unwanted packets, unfriendly login attempts, and DoS attacks before even authentication process begins.

P60

SPTK16

Anti-virus, Anti-

spyware and Anti­adware in App Layer

Security software like antivirus or anti spyware is important for the reliability, security, integrity and confidentiality of the IoT system.

P60

SPTK17

Autonomic cyber

security managemen t framework

To follow this tactic the [p81 can be applied. This work introduces an autonomic model-based cyber security management approach for the Internet of Things (foT) ecosystems. The approach aims at realizing a self-protecting system, which has the ability to autonomously estimate, detect, and react to cyber attacks at an early stage. The approach integrates various model-based techniques including: 1) real-time estimation and baseline security controls to predict and eliminate potential cyber attacks; 2) data analysis to identify and classify attacks; and 3) a multicriteria optimization method to select the optimal active response for deploying countermeasures while maintaining system functions. The prototype framework has been developed with a master controller virtual machine, which can be configured for various platforms. Besides estimating, detecting, and protecting against known attacks, the approach can also learn signatures of unknown attacks in real time. Unknown attacks are identified for future protection by updating detection algorithms with the underlying signatures. In our framework design, the main protection modules are installed on the MC-VM, which ensures that the self-protection mechanism continues to work even if the underlying system is compromised. A multitier web application case study is presented. Our self-protecting system successfully secured the web atm from various known and unknown attacks. Below is a figure of main components of the autonomic security management framework. More details in [p8].

P8



Clients t­

bwironment
  
model

w

RallrecOon
  
module

NeL fnorm

" I MeI

n

Sensors

ten dad.

p.

Model
  
kw -1
  
Prixtv

Security
  
model

Adyeisaies

Routs

legitimate packet

Pe•

Enown malicious

Imams

Most data pre-
  
processing

' module

MC-VM

Ru

upd



ntom

model classifier State Security status (Normal/Ab orn all

FOttlif lint
  
process

Know
  
attoc

Data
  
sensors

X

Model library

VM data



Protection

j:

6E".

,

tea Nig

Is

Fuzzy /Oak
  
controller

Data pre. PeOCCessing

PROMETHEE 11 I

pdates

|  |  |  |  |
| --- | --- | --- | --- |
|  | | | |
| I Performance I  ios | 'Signature'  IDS | Pet ton hbea |  |
|  | | | |

Test da a

Criteria

Performance
  
IDS

Utility funs

'Prof

function;

Main host

nAlnknown)

SPTK18

Classical counter­measures for Self-protection

Security solutions have been classified as either self-protecting or self-healing, in relation to the autonomic mechanism used for mitigation. Self-protecting solutions follow a passive approach and attempt to prevent security threats before they happen. This is done using various cryptographic techniques, with the knowledge of how common attacks are executed. In the case of self-healing solutions, the specific counter-measures for mitigation are taken only after the attack has been detected. Reactive measures are easier to achieve than protective measures, as typically the attacks aim confidentiality, integrity, availability, authenticity or privacy. Nevertheless, it is important to include protective mechanisms as well supplementing the reactive mechanisms, resulting in what we call as hybrid schemes. In [p15] is presented countermeasures.

P15

SPTK19

Enhance location privacy

Vast deployment will make RFID a pervasive technology. Thus, security and privacy are import issues to be considered. Many location-aware applications emerge; systems are capable of tracking all of our movements and recording anything. This is done in the name of convenience or due to economic reasons. Legislation must ensure that privacy of the individual is still protected; researchers must develop the required techniques. An overview of current approaches for enhancement of privacy has been given above and their capability of handling the various threats RFID faces has been explained. The [p24] proposed a hash-
  
based scheme with a high inherent security rendering it a useful technique for all kinds of applications where static identifiers are used currently and location privacy is an issue. The main benefit of the proposed scheme is its simplicity: It only requires implementation of a hash function in the tag and data management at the backend and does not rely on random numbers generated by the tag, strong symmetric or even asymmetric encryption. It offers a high degree of location privacy and is resistant to many

forms of attacks like eavesdropping. Further, only a single message exchange is required, the communications channel need not be reliable, the reader/third party need not be trusted, and no long-term secrets need to be stored in tags. Most of the denoted drawbacks have already been solved and the solutions will be published in subsequent publications.

P24

SPTK20

Countermea sures for Time

Synchroniza tion Attacks

In [P28] is proposed countermeasures for single hop networks and multi-hop networks separately. Each time synchronization protocol facilitates single hop synchronization by having a node periodically broadcast its local version of the global time and allowing the other nodes to synchronize their docks to that time. Since multihop time synchronization algorithms are all extensions to that basic building block, our proposals for multihop networks are a superset of our proposals for single hop networks.

P28

SPTK21

Routing Protocol

AODV, DSR, TORA and OLSR ad-hoc routing protocols.

P29

SPTK22

Threshold Cryptograp by-based Group Authenticati

Internet of things (IoT) is an emerging paradigm where the devices around us (persistent and non-persistent) are connected to each other to provide seamless communication, and contextual services. In the IoT, each device cannot be authenticated in the short time due to unbounded number of devices. Equally, it is difficult to get receipt of their authentication request at the same time. Therefore, secure, and efficient group authentication scheme is required that authenticates a group of devices at once in the context of resource constrained IoT. The [p30] presents novel Threshold Cryptography-based Group Authentication (TCGA) scheme for the IoT which verifies authenticity of all the devices taking part in the group communication. The proposed TCGA scheme is implemented for WIFI environment, and the result shows that TCGA scheme is lightweight, and alleviates the effect of battery exhaustion attack. The [p30] also presents time analysis, and formal security analysis of TCGA scheme which shows that the proposed TCGA scheme is safe from the replay, man-in-the-middle attack, and is scalable in nature.

P30

on

SPTK23

SybilLimit

Decentralized distributed systems such as peer-to-peer systems are particularly vulnerable to Sybil attacks, where a malicious user pretends to have multiple identities (called sybil nodes). Without a trusted central authority, defending against sybil attacks is quite challenging. Among the small number of decentralized approaches, the recent SybilGuard protocol of [p38] leverages a key insight on social networks to bound the number of sybil nodes accepted. Although its direction is promising, SybilGuard can allow a large number of sybil nodes to be accepted. Furthermore, SybilGuard assumes that social networks are fast mixing, which has never been confirmed in the real world. The [p38] presents the novel SybilLimit protocol that leverages the same insight as SybilGuard but offers dramatically improved and near-optimal guarantees. The number of sybil nodes accepted is reduced by a factor of Q06), or around 200 times in our experiments for a million-node system. We further prove that SybilLimit's guarantee is at most a log n factor away from optimal, when considering approaches based on fast-mixing social networks. Finally, based on three large-scale

real-world social networks. the 1D381 provide the first evidence that real-world social networks are indeed fast mixing. This validates the fundamental assumption behind SybilLimit's and SybilGuard's approach.

P38

SPTK24

SybilGuard

Peer-to-peer and other decentralized, distributed systems are known to be particularly vulnerable to sybil attacks. In a sSil attack, a malicious user obtains multiple fake identities and pretends to be multiple, distinct nodes in the system. By controlling a large fraction of the nodes in the system, the malicious user is able to "out vote" the honest users in collaborative tasks such as Byzantine failure defenses. This paper presents SybilGuard, a novel protocol for limiting the corruptive influences of sybil attacks. Our protocol is based on the "social network" among user identities, where an edge between two identities indicates a human-established trust relationship. Malicious users can create many identities but few trust relationships. Thus, there is a disproportionately-small "cut" in the graph between the sybil nodes and the honest nodes. SybilGuard exploits this property to bound the number of identities a malicious user can create. We show the effectiveness of SybilGuard both analytically and experimentally.

P39

SPTK25

The [p90] proposed a Lightweight Defense Scheme against Selective Forwarding Attacks in Wifeless Sensor Networks that can be used in IoT application. According to characteristics of easy positioning the nodes around transmission paths in a structured topology made of hexagonal mesh, the nodes around transmission path are used to monitor packet transmission of its neighbor nodes, judge the attackers' location and resend the packets dropped by the attackers. The method is effective in detecting selective forwarding attacks to ensure reliable packet delivery. Analysis and simulation results show that the proposed scheme consumes less energy and storage. More details in [p90].

Advantages:

* The routing discover scheme is dynamically generating path which makes adversary difficult to launch attack.
* There is no traffic overhead to detect malicious node.
* Neighbour nodes are judging the malicious nature of a node, so no need of shared key between every two nodes in the network, which reduces storage required.
* Efficient utilization of energy since only one node is active at a time in each RC.

Drawbacks:

* How much trustworthy a monitor node is?
* If a node is malicious, the scheme did not explain whether to remove complete RC or only that node from routing discovery process. If we are removing complete RC then not efficient resource utilization.
* Routing is a probability based one which is not an optimal one.
* We require GPS to acquire the locations of nodes which makes network costly.

P45

P90

Lightw eight Defense scheme

SPTK26

Multi Data Flow

Scheme

Multi Data Flow Scheme is a single scheme which defends against selective forwarding

attack. The scheme uses multiflow topologies to defend the attack. In multi-dataflow scheme, the whole network is divided into different data topologies that makes, a sensor node belonging to one topology can communicate and send information only through nodes of the same topology. This division can be done at different times. Generally division takes place at deployment time. If not then the nodes can randomly choose a topology number after deployment phase.

The condition in this scheme is that every topology has to cover the sensing area completely. More details in [p91]. Advantages Of this Scheme:

* In this scheme no need of any additional hard-ware/software is needed to mitigate the attack.
* There won't be any packet loss or delay due to attack due to which packet delivery ratio will be high.

Drawbacks:

* Network cost is high.
* Network lifetime will be low since due to multi data transmission.
* If attack occurs in all topologies then there wont be any defend from attack

P45

P91

SPTK27

Flooding Attack Prevention.

To defend routing protocols against the Ad hoc Flooding attack, we develop a generic secure component, called Flooding Attack Prevention (FAP) which can be applied to AODV routing protocol to allow that protocol to resist the rushing attack. Flooding Attack Prevention (FAC), a generic defense against the Ad hoc Flooding Attack. When the intruder broadcasts exceeding packets of Route Request, the immediate neighbors of the intruder record the rate

of Route Request Once the threshold is exceeded, nodes deny any future request packets from the intruder. More details in [p49].

P49

SPTK28

Vulnerabilit y scans

Mitigation solutions include constant vulnerability scans using ma ware pattern classification [p50] and risk mitigation services. The pattern classification can be done using the autonomic control loop component of "Analysis" following which the autonomic "execution" of the mitigation service can be performed.

P50

SPTK29

Clustering protocols

Clustering protocols can be used agonist to failures and attacks. The Perfectly anonymous data aggregation protocol [p92] can be used in IoT Application. Clustering and data aggregation in wireless sensor networks improves scalability, and helps the efficient use of scarce resources. Yet, these mechanisms also introduce some security issues; in particular, aggregator nodes become attractive targets of physical destruction and jamming attacks. In order to mitigate this problem, [p92] propose a new private aggregator node election protocol that hides the iclerwsyit of the elected aggregator nodes both from external eavesdroppers and from compromised nodes participating in the protocol. [p92] also propose a private data aggregation protocol and a corresponding private query protocol which allows the aggregators to collect sensor readings and respond to queries of the base station, respectively, without revealing any useful information about their identity to external eavesdroppers and to compromised nodes. Others Clustering protocols are discussed in [p51] and can be applied in IoT applications.

P51

P92

SPTK30

Risk Assessment

It is fundamental for the continuing security of the system, by discovering new threats, applying

Updates and patches to the firmware on the system devices, as well as providing improvements in the existing security structure. Risk Assessment: b) Finding New Threats, c) Applying Updates

d) Applying Patches, e) Providing Improvements and 0 Upgrading Systems.

P60

SPTK31

Securing the

premises

Securing the premises is perhaps the most important security feature that IoT needs, as it physically secures the IoT devices; i.e. sensor nodes, computers, firewalls, data servers

etc. The security of the IoT devices is achieved by using Physical Barriers to block any unauthorized people, Intrusion Detection Systems to monitor any strange behavior, Access

Control to make sure only legible users enters the premises of the IoT and even Security personnel to ensure total security of the IoT devices.

Securing the IoT Premises:

1. Physical Bathers
2. Intrusion Detection Alarms
3. Monitoring Devices
4. Access Control Devices
5. Security Personnel

P60

SPTK32

IEEE Standards Solutions

The IEEE provides standard mechanisms for the physical (PHY) and medium access control (MAC) layers which are useful in implementation of a smart city. There exist three families that can provide low-power and short-range IoT operation for a smart city [7].

IEEE 802.15.4:

Important characteristics include real-time quality by guarantying time slots, collision dodging through CSMA/CA and merged assistance for secure communication. Moreover, the devices include power management functions for example, energy detection and link quality. IEEE 802.15.1 is used in Bluetooth. IEEE 802.15.11 This technology is provided from Wi-Fi Alliance, a trade association in control of the certifying products if they adjust to particular standards of interpret-ability. The Wi-Fi Protected Access (WPA) [56] is a security protocol that has become the regulation for providing security .11 networks. Here by using an already shared encryption key (PSK) or digital certificates, the WPA algorithm Temporal Key Integrity Protocol (''KIP) encrypts information providing authentication to the particular

networks. he WPA algorithm (TKIP) further improved upon to the new WPA2 [571 [561 that utilize more securer encryption algorithm that is Advanced Encryption Standard (AES). Moreover this protocol also uses better

and advanced key distribution techniques, which help in improved session security to avoid eavesdropping.

P111

SPTK33

Tag blocking, Tag

sleeping and

Selective blocking

It is important to discuss various techniques and strategies that may play part in better security performance of RFID in a smart city. Privacy protection is an important need and right of the citizens and as discussed previously, that tag killing may play role in privacy protection but this also may lead to loss data permanently. A better option is tag sleeping. When the tag does not need to to be read, it is put to sleep temporarily [45]. There is another concept of tag blocking and selective blocking [40].

P111

SPTK34

Re-encryption and

minimalist cryptograph

y

Privacy protection is an important need and right of the citizens and as discussed previously,

that tag killing may play role in privacy protection but this also may lead to loss data permanently. Other techniques include relabeling approach, re-encryption and minimalist cryptography [45].

P111

SPTK35

Data coding and

multiple re transmissio n

The interference problems in the RFID system can be dealt by data coding, multiple re transmission and data integrity check.

P111

SPTK36

Hash-Lock and Hash Link

Hash-Lock and Hash Link techniques are also important as they provide better authentication. There are other authentication techniques based on hash such as ID exchange and distributed RFID challenge/answer authentication [39].

P111