Term Project CS549 Jan-May 2022

Course Instructor: **Prof Sukumar Nandi**
Abstract submission deadline: 14th February 2022
Proposal submission deadline: 4th April 2022

The term project is a maximum 12 page and a minimum 6-page research paper. The paper should be in pdf of IEEE double-column format. You are advised to use latex to prepare the paper. The latex styles and another basic toolbox for IEEE double column format can be obtained from https://ieeeauthorcenter.ieee.org/. The paper should examine issues or technologies related to network security. Typically, your report might be organized as follows:

1. Abstract
2. Introduction
3. Related Work
5. Analysis and Experiments
6. Result and Discussion
7. Conclusion and Future Work
8. References

The paper will be graded on the quality of research, quality of experiments, quality of results, quality of presentation, and strength of references. Original research counts more than a critical review, which counts more than a mere survey paper. Implementing and testing things counts more than reporting on someone else's experiments/results. A list of possible topics is given in this document along with the TAs, but you may suggest your own. **You need to contact one of the TAs and discuss about your topic before submitting the abstract. Marks are allocated for in-time abstract submission.** You need to submit the abstraction to the respective TA, and the final report into Moodle. Please submit your term paper reports (abstract and final) in pdf format with the name format <rollnumber>.pdf. **Reports will undergo plagiarism check and similarity more than 20% will result into zero mark.**

Below are the suggested topics.

Internet of Things (IoT) and its Security

TA: Pradeep Kumar Bhale : pradeepkumar@iitg.ac.in
Saurav Kumar : ksaurav@iitg.ac.in

There has been a tremendous growth in the number of smart devices and their applications (e.g., smart sensors, wearable devices, smart phones, smart cars, etc.) in use in our everyday lives. This is accompanied by a new form of interconnection between the physical and digital worlds, commonly known as the Internet of Things (IoT). This is a paradigm shift, where anything and everything can be interconnected via a communication medium. In such systems, security is a prime concern and protecting the resources (e.g., applications and services) from unauthorized access needs appropriately designed security and privacy solutions.

1. **Link for Basics about IOT:** https://drive.google.com/file/d/15CKBelMgFqLjrcFUc73NFfisSrKiHPTu/view?usp=sharing
2. **Link for different vulnerabilities in IOT:** https://drive.google.com/file/d/1nR47GRv5ukYf91FpeMzdrrQUV2RQCAzS/view?usp=sharing

Abstract Research Topics:

1) Non-Cooperative Game to Balance Energy and Security in IoT Networks
https://ieeexplore.ieee.org/abstract/document/9162702
2) A Multi-Layer Security Monitoring System for IoT Networks
https://ieeexplore.ieee.org/abstract/document/9155424
https://link.springer.com/chapter/10.1007/978-3-642-32427-7_54
3) A hybrid machine learning approach for detecting Botnet attacks in IoT ecosystem.
https://link.springer.com/chapter/10.1007/978-981-16-8059-5_19
4) Low-Rate DDoS Attacks in IoT network
https://ieeexplore.ieee.org/abstract/document/8794618
https://www.inderscienceonline.com/doi/abs/10.1504/IJSNET.2020.109720
5) The Security Perspective: Fog-enabled IoT
https://www.sciencedirect.com/science/article/pii/S0167739X18323367
6) Fractal Analysis based Detection of DDoS attack in IoT ecosystem
https://ieeexplore.ieee.org/abstract/document/8867618
7) AI-empowered IoT Security for Smart Cities
https://dl.acm.org/doi/abs/10.1145/3406115
8) Detection and prevention of routing attacks in IoT
https://ieeexplore.ieee.org/abstract/document/8456088
9) A Security Design for the Detecting of Buffer Overflow Attacks in IoT Device
https://ieeexplore.ieee.org/abstract/document/8536378
10) Large-scale reflection DDoS attacks detection and mitigation in IoT ecosystem
https://www.tandfonline.com/doi/full/10.1080/00051144.2021.1885587
11) Security Issues in the Routing of IOT
https://drive.google.com/file/d/1vimcSXb0svEWIe0_1Wi8cYsqj2WSZgKN/view?usp=sharing
12) Intrusion Detection in IOT using Machine learning:
https://drive.google.com/file/d/1vimcSXb0svEWIe0_1Wi8cYsqj2WSZgKN/view?usp=sharing
https://drive.google.com/file/d/1017jnZxCGhSm-HEOkQ1oMlZvnI-LqfZ8/view?usp=sharing

Security Issues in Device-to-Device (D2D) Communications

TA: Manoj Das (mdas@iitg.ac.in)

In Cellular Networks, Device-to-Device (D2D) communication allows direct communication between two devices, without the participation of the Base Station. It promises improvement in energy efficiency, throughput, delay and has the potential to effectively offload traffic from the network core.

Basic Overview: https://en.wikipedia.org/wiki/Device-to-device

1. Detection and Prevention of attacks in D2D Communications

In conventional cellular communication, the UE is first identified, authenticated and then encryption of the radio link occurs. The core network is a trusted party. But this is not the Case in D2D communication as transmission occurs without the assistance of the core network. Also, wireless channels are broadcast in nature. As a result, they are susceptible to a number of attacks, including the ones mentioned below:

-Man in the Middle: The malicious node acts as a client for the server and a server for the client, i.e. a D2D receiver to the D2D transmitter and vice-versa.
-Node Impersonation: Malicious node acts as a legitimate node, posing threat to D2D communication.
-Denial of Service: Attempt to make resources unavailable for authorized UEs.
-Eavesdropping: Unauthorized interception of the confidential data between the DUEs.

Reference Paper: https://www.sciencedirect.com/science/article/pii/S1084804516302727

2. Authentication Mechanisms for D2D communications

Authentication is the process of verifying the identity of a user, process, or device, often as a prerequisite to allowing access to resources. 3GPP, in it's D2D specifications, has not provided recommendations about how mutual authentication, device anonymity, and message non-repudiation are guaranteed. To overcome all these security challenges, there is a need to design a secure way to protect D2D network traffic: it should mutually authenticate two parties and exchange information without revealing anything to adversaries.

Reference Paper: https://ieeexplore.ieee.org/document/8122069

Security and Trust management in Peer to Peer networks

TA: Debanjan Roy Chowdhury (chowdhur@iitg.ac.in)

The peer-to-peer (P2P) movement allowed millions of Internet users to connect "directly, forming groups and collaborating to become user-created search engines, virtual supercomputers, and filesystems. This model of network arrangement differs from the client–server model where communication is usually to and from a central server. Peer-to-peer networks generally implement some form of virtual overlay network on top of the physical network topology, where the nodes in the overlay form a subset of the nodes in the physical network. BitTorrent is one prominent example of P2P network. Peer-to-peer systems pose unique challenges from a computer security perspective. Like any other form of software, P2P applications can contain vulnerabilities. Lack of any centralized control over the network, and the dynamic availability of peer nodes make the detection of security threats extremely challenging making the network vulnerable. Some of the well-known threats are sybil attack, routing table attack, message forwarding attack, DDoS, etc. Some survey papers on these attacks and recent research trends are given below.

Survey:

https://link.springer.com/chapter/10.1007/3-540-36532-X_4

https://ieeexplore.ieee.org/abstract/document/4796923

Botnet detection and mitigation in P2P networks

https://link.springer.com/article/10.1007/s00521-016-2564-5

https://ieeexplore.ieee.org/abstract/document/8524529

https://ieeexplore.ieee.org/abstract/document/9237706/authors#authors

https://ieeexplore.ieee.org/abstract/document/8854561

Trust management in P2P networks

To mitigate the threats mentioned above, trust management among nodes are extremely important. As there is no centralized entity to implement trust system, a distributed trust system needs to be realized through reputation management which is one of the trending topic in P2P system. Few examples are given in the below links.

https://ieeexplore.ieee.org/abstract/document/6514820

https://ieeexplore.ieee.org/abstract/document/4159793

https://www.sciencedirect.com/science/article/pii/S1389128615002340

Vehicular Networks and its Security

TA: Debanjan Roy Chowdhury (chowdhur@iitg.ac.in)

Primary motivation of vehicular network or VANET is to save on-road human lives. For that purpose, vehicles periodically sense their surrounding data through various sensors and shares among neighbour vehicles, as well as to central server for analysis and mining purpose. Based on these received data, vehicles and central nodes can take appropriate decisions for smooth functioning of vehicle traffic. With these benefits of VANET, there are major vulnerabilities too. Malicious or selfish vehicles can generate false reports to deceive the system into their favour or to simply destroy the system like issuing false accident alarm or falsely reporting congestion message. Detailed survey of the security threats and vulnerability of VANET is given in the below links:

https://www.sciencedirect.com/science/article/pii/S2214209619302268

https://ieeexplore.ieee.org/abstract/document/8345196

Privacy, anonymity, and trust management of VANETs

To mitigate message falsification, vehicles must be held responsible for their actions and must be made face the legal consequences. For that it requires each vehicle to attach their identities with each sent message by digitally signing them. But that creates the location privacy issue. Vehicle owners do not want to reveal their visiting locations and do not want to be tracked. They prefer complete anonymity with the peer vehicles except with legal authorities. On the other hand, lack of identity, or spoofed identity leads to lack of trust among peer vehicles which can prevent the system to work properly. To mitigate these challenges, researcher has come up with various novel trust management system which builds trust among peer vehicles while maintaining the anonymity of individual vehicles making them untraceable. Few of the recent researches in this direction are given below:

https://ieeexplore.ieee.org/abstract/document/8920075

https://ieeexplore.ieee.org/abstract/document/8455893

https://ieeexplore.ieee.org/abstract/document/9262037

Routing attacks in Vehicular Networks

Even though trust management systems can secure the application layer messages, network layer messages are still vulnerable and can pose significant threats and can put the system down. Few examples are black-hole attacks, worm-hole attacks, DDos attack, etc. Honest vehicles can collectively detect such attacks and can mitigate them in some extent. Recent research topics are given in the below links:

https://www.sciencedirect.com/science/article/pii/S0141933120305111

https://ieeexplore.ieee.org/abstract/document/5403263

https://ieeexplore.ieee.org/abstract/document/6514286

https://ieeexplore.ieee.org/abstract/document/8935220

Blockchains and its Applications

TA: Saurav Gupta (g.saurav@iitg.ac.in)

Distributed Consensus

Blockchain is a form of distributed ledger that is capable of immutability, and has many more added benefits. Though is was first used in Bitcoin cryptocurrency, the blockchain technology has become a framework by itself which is able to support various kinds of distributed applications like Daaps, Smart-contract, etc. In the heart of every blockchain there is a consensus algorithm through which all nodes agree on a single state of the system. Various kinds of consensus algorithms like PoW, PoS, PoA, etc. are in practise depending on the demand of the system. Given below the recent researches related to distributed consensus and suggested improvements.

https://ieeexplore.ieee.org/document/8972381

https://ieeexplore.ieee.org/abstract/document/8516911

https://ieeexplore.ieee.org/abstract/document/9461057

Access control for IoT:

Access control is a fundamental component of data security that dictates who's allowed to access and use company information and resources. Through authentication and authorization, access control policies make sure users are who they say they are and that they have appropriate access to company data. Access control can also be applied to limit physical access to campuses, buildings, rooms, and data-centres.

https://ieeexplore.ieee.org/document/8968396/

Access control of IoT can be done using Blockchain framework.

https://ieeexplore.ieee.org/abstract/document/8766453/