



NetSpect

KVH-015: Mesh Network Detection
Enabling Cyber Intelligence through SaaS



Shifu's Squad

Ghanashyam Bhat

Karan Bhat Sumbly

Prajwal Bhat

Vijit Kumar

Niveditha Kundapuram

Adarsh Kumar

Illicit Usage of Mesh Networks

Where there's GOOD, there's BAD

Problem



No connectivity with cellular networks

No requirement to connect to the Internet



Similar frequency range as Wi-Fi and Bluetooth

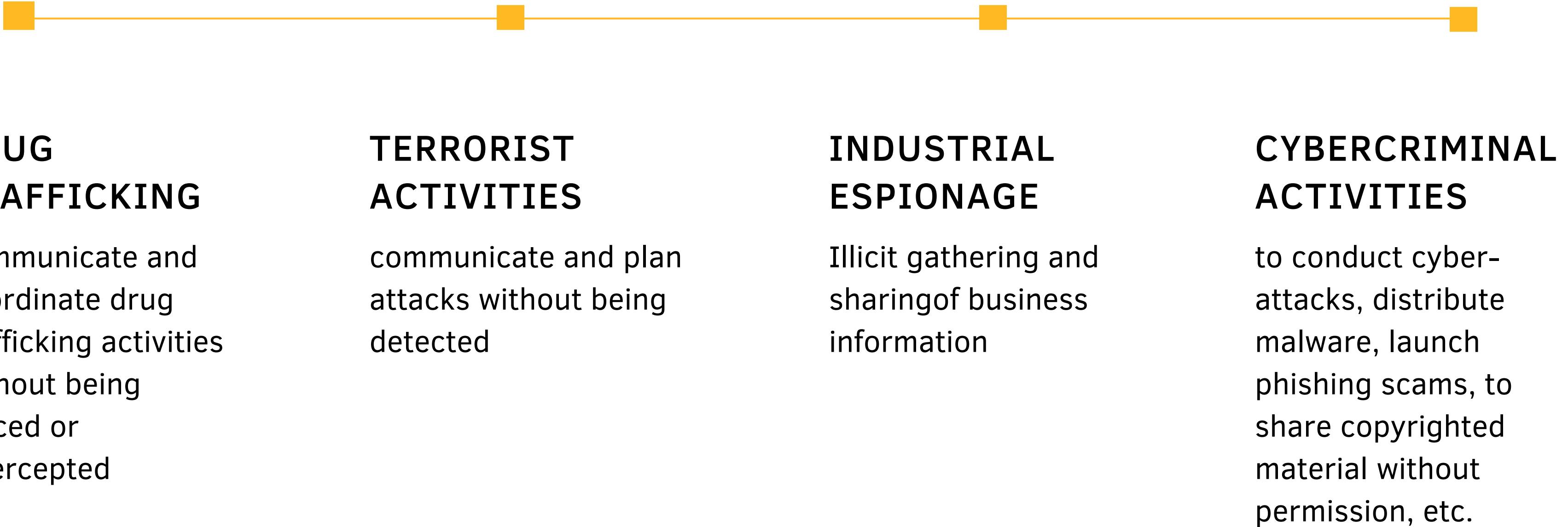
Makes distinguishing mesh network packets difficult



Dynamic status of nodes

Nodes leave and join the network dynamically; difficult to track

Existing Scenario



Utopia



Creation of private mesh network

- configured network interfaces to Ad-hoc mode
- Nodes configured to the same cell number



Wi-Fi vs Mesh Ad-hoc Packet Analysis

- Additional MDNS layer (active)
- Broadcast Properties: identify properties to differentiate



Statistical Network Analysis

- Traffic pattern and network usage
- Deduce potential threats
- Disrupt network

Activities Google Chrome Mar 19 11:58 AM 100 %

Login 127.0.0.1:5000/scan

Work PES College Social Media Resources Projects Placement Competitions Security Movies and So... Other

Join Mesh Ping Scan

Networks in the range

Filter

Name	Type	Security
Kavach	Ad-Hoc	WEP
LAPTOP-US4OAP2P	7013	WEP
GJBC_Cafeteria	Infra	--
26:15:10:29:02:42	GJBC_PESU52	WEP
GJBC_Cafeteria	Infra	--
GJBC_PESU52	Infra	--
--	Infra	WPA2
	Infra	WPA2

127.0.0.1:5000/scan-filter

Demonstration

Activities Google Chrome Mar 19 11:58 AM 100 %

Login 127.0.0.1:5000/scan-filter

Work PES College Social Media Resources Projects Placement Competitions Security Movies and So... Other

Join Mesh Ping Scan

Networks in the range

Filter

Name	Type	Security
Kavach	Ad-Hoc	WEP

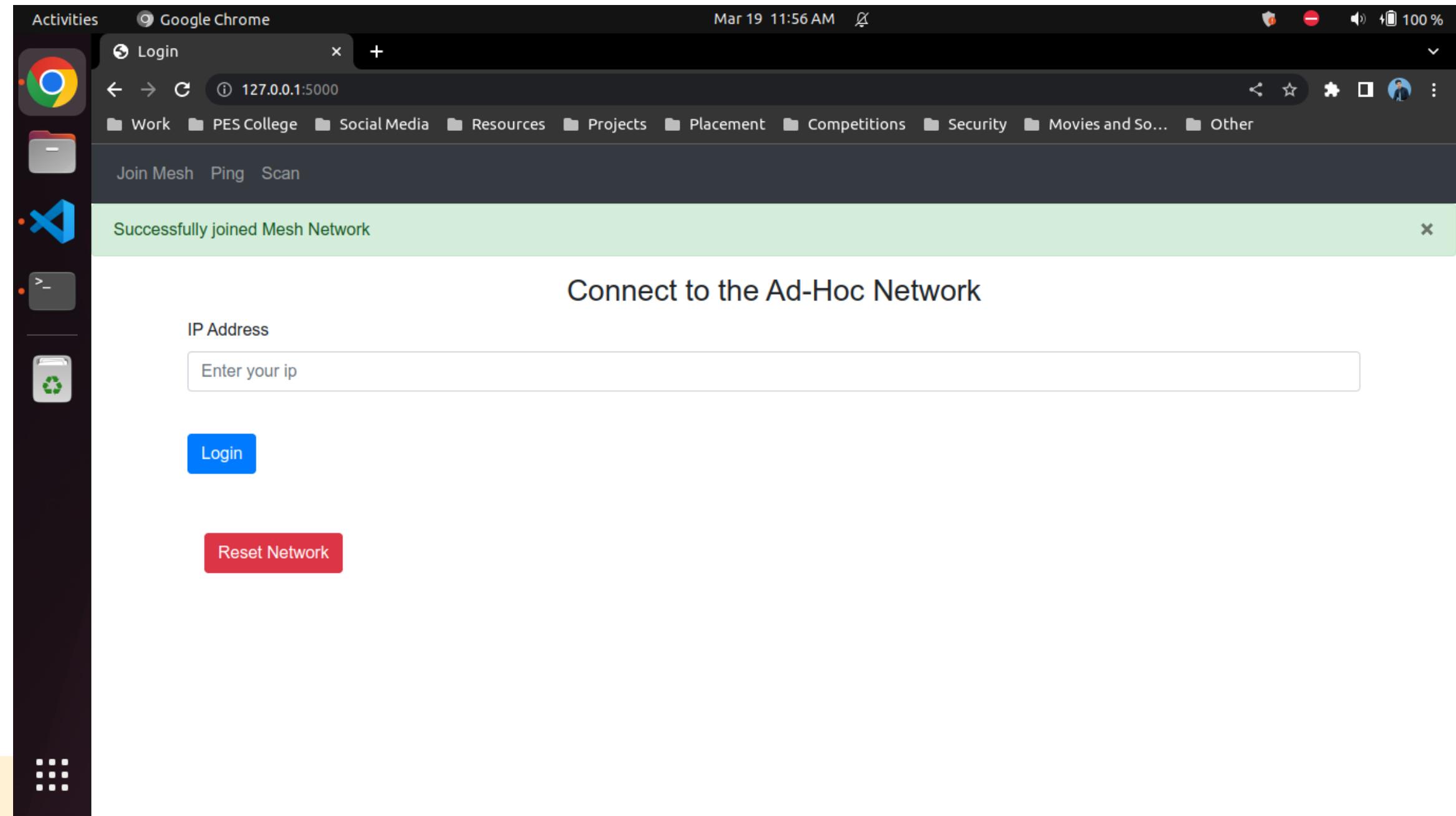
127.0.0.1:5000/scan-filter

[00:00:00] Tested 127062 keys (got 10451 IVs)

KB	depth	byte(vote)
0	1/ 23	12(15104) E0(14848) 2D(14336) 23(14080) B1(13824) 39(13568) 69(13568) 7C(13568) B9(13568) 09(13312) 43(13312)
1	0/ 2	34(17408) A8(14848) 1C(14592) 85(14592) F1(14592) BB(14336) F3(14336) 86(14080) B1(14080) 2C(13824) 7E(13824)
2	6/ 25	56(14080) 01(14080) 42(13824) 5F(13824) 0A(13824) 26(13824) 38(13568) AD(13568) DA(13568) 75(13312) BF(13312)
3	10/ 12	C8(13312) 14(13056) 3C(13056) 69(13056) 6A(13056) 8A(13056) 1A(12800) 2B(12800) 64(12800) 68(12800) 83(12800)
4	0/ 10	90(16128) 12(15360) D4(15104) B8(14848) 20(14592) C3(14592) CE(14336) AC(14080) 2F(13824) C0(13824) 36(13568)

KEY FOUND! [12:34:56:78:90]

Decrypted correctly: 100%



Demonstration

Activities Google Chrome Mar 19 11:57 AM 100 %

Login 127.0.0.1:5000/ping

Work PES College Social Media Resources Projects Placement Competitions Security Movies and So... Other

Join Mesh Ping Scan

Successfully sent 5 ICMP packets

Ping to the IP Address

IP Address

Enter destination ip

Ping

Start Network Analysis

127.0.0.1:5000/analyse

This screenshot shows a desktop environment with a dark-themed window manager. A browser window titled 'Login' is open at the URL '127.0.0.1:5000/ping'. The page contains fields for entering an IP address and a red 'Ping' button. Below these is a yellow 'Start Network Analysis' button. To the right, a separate window titled '127.0.0.1:5000/analyse' displays a chart titled 'Figure 1' showing 'Network Traffic' over time. The chart has 'Packet Count' on the y-axis (0 to 160) and 'Time' on the x-axis (0 to 30). The data series shows a sharp peak at time 10 with approximately 160 packets, followed by a gradual decline.

Time	Packet Count
0	0
5	80
10	160
20	80
30	65

Demonstration

A photograph showing three people working together on a laptop. A woman with curly hair and a yellow top is on the left, looking up. A man with glasses and a tan jacket is in the center, pointing at the screen. Another man with braided hair and glasses is on the right, also looking at the screen. They are all wearing casual to semi-casual attire. The background is a plain white wall.

Target Market

■ Armed Forces & Law Enforcement Agencies

- Police
- Border Security Force (BSF)
- Anti-Naxalite Forces (ANF), Special Task Forces (STF) and Commando Battalion for Resolute Action (CoBRA)

■ Institutions & Business Organisations

- Offices, universities, etc

Revenue



The State and Central Governments

Half-annual and annual based subscriptions - region specific

Institutions & Business Organisations

SaaS based payments



Future Roadmap



STEP 1

Develop more robust algorithms for packet classification

STEP 2

Use GPU for brute force password cracking

STEP 3

Implement GIS to get precise location of nodes

STEP 4

Prototype conversion to portable devices

Technical Details

Application

locally deployed



Front-end

- HTML/CSS
- Jinja



Password Decryption

- Aircrack-ng
- Monitor Mode Adapter



Back-end

- Flask
- Shell Scripting
- Python
- Networking Frameworks

The Team

