PROJET INDIVIDUEL

SYSTÈMES DE DÉTECTION D'INTRUSION POUR L'INTERNET DES OBJETS

Présenté par Théo Plockyn et Rémy Debue

PLAN DE LA PRÉSENTATION

Contexte général

Contexte spécifique

Projet et focus sur une partie

INTRODUCTION

Cadre de nos études

Curieux de la sécurité

Recherche : équipe 2XS

Institut de **r**echerche sur les **c**omposants logiciels et matériels pour l'**i**nformation et la **c**ommunication **a**vancée de Lille

Hôtel à projets interdisciplinaires.

Recherches centrées sur l'intelligence ambiante.

EQUIPE 2XS

eXtra Small eXtra Safe

Encadré par Gilles Grimaud

Projet sur la sécurité des réseaux

LE SUJET

Systèmes de détection d'intrusions
pour l'Internet des objets

SYSTÈME DE DÉTECTION D'INTRUSIONS

Aussi appelé IDS

Repérer des activités anormales sur un réseau

Connaissance des tentatives d'intrusions réussies comme échouées

INTERNET DES OBJETS

Aussi appelé IoT

Extension d'Internet au monde physique

Utilisations diverses et variées

LA SÉCURITÉ DANS L'IOT

Sécurité réelle faible actuellement

Systèmes embarqués contraints

Besoin solutions de sécurité adhoc

SÉCURITÉ : POURQUOI C'EST DIFFICILE ?

Attaques passives

Attaques actives

OUTILS POUR IDS

Capter les informations : Sonde

Vérifier les informations : Discus

DISCUS

Projet de l'équipe 2XS

Framework d'IDS

NOTRE SONDE

Contiki

6LoWPAN

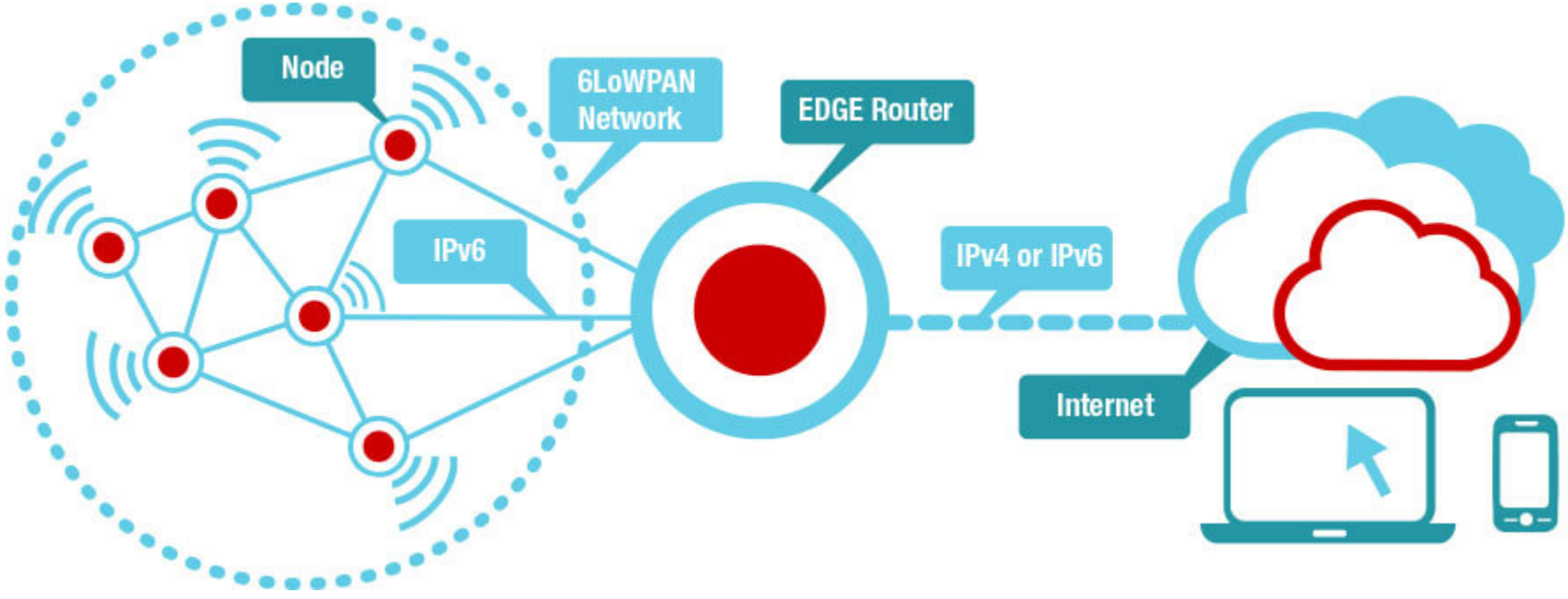
CONTIKI

Système d'exploitation embarqué

Léger et flexible

Possède beaucoup de caractéristiques d'OS habituels

6LOWPAN


Node
6LoWPAN
Network
EDGE Router
IPv6
IPv4 or IPv6
Internet

Norme sur les communications en IPv6

Orienté vers l'informatique embarquée

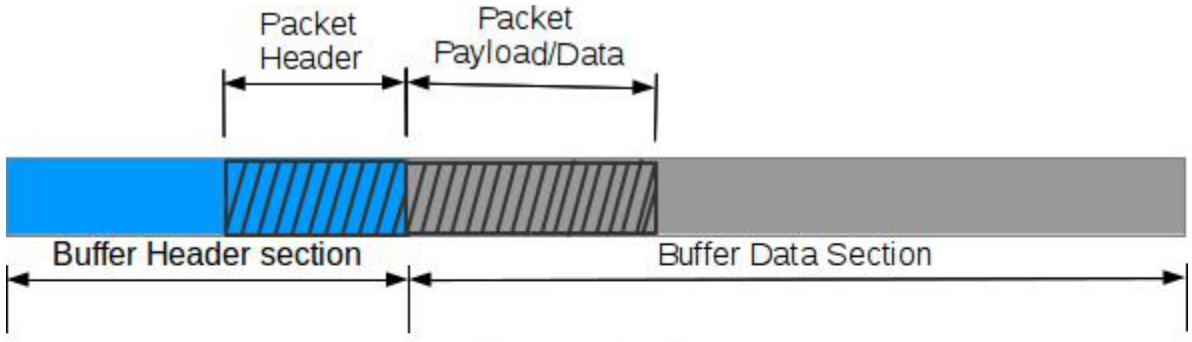
Augmentation de la charge utile : headers compressés

TRAITEMENT DES PAQUETS DANS CONTIKI

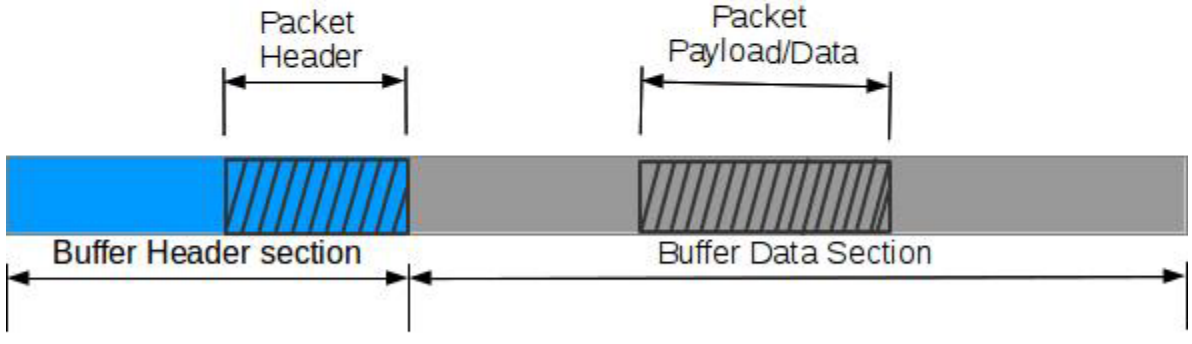
Différence entre paquets entrants et sortants

Parsing des paquets

DIFFÉRENCE ENTRE PAQUETS SORTANTS ...



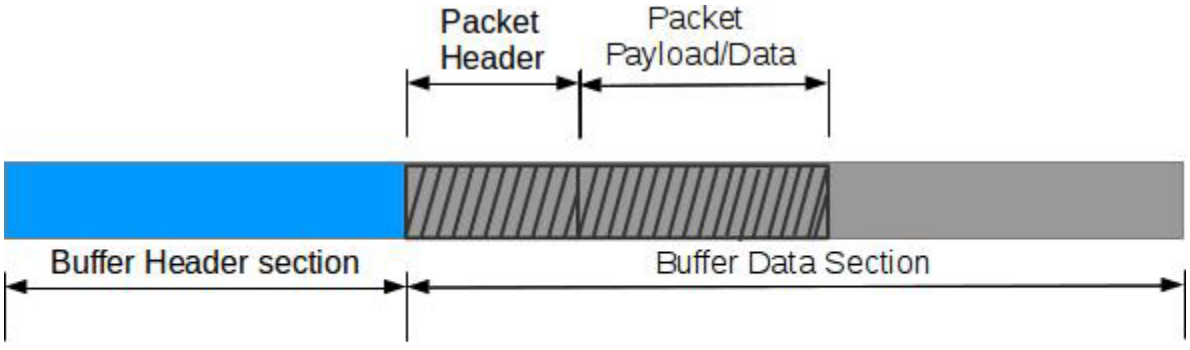
Scenario 1



Scenario 2

Outbound Packet

ET ENTRANTS



Inbound Packet

TRAITEMENT DES PAQUETS

Tri des paquets

Bit Pattern	Short Code	Description
00 xxxxxx	NALP	Not A LoWPAN Packet
01 000001	IPv6	uncompressed IPv6 addresses
01 000010	LOWPAN_HC1	HC1 Compressed IPv6 header
01 010000	LOWPAN_BC0	BC0 Broadcast header
01 111111	ESC	Additional Dispatch octet follows
10 xxxxxx	MESH	Mesh routing header
11 000xxx	FRAG1	Fragmentation header (first)
11 100xxx	FRAGN	Fragmentation header (subsequent)

CONCLUSION

MERCI DE VOTRE ATTENTION

DES QUESTIONS ?